GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

A Framework for Managing Fraud Risks in Federal Programs

July 2015

GAO-15-593SP

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.

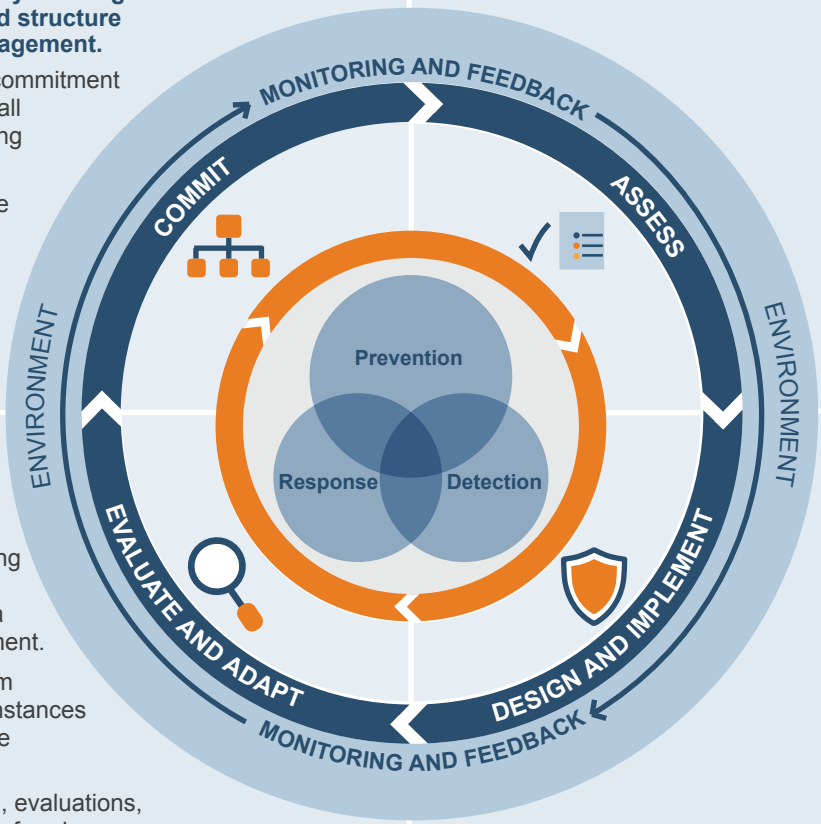
The Fraud Risk Management Framework and Selected Leading Practices

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

Contents

Tables

Figures

Abbreviations

ACFE	Association of Certified Fraud Examiners
CMS	Centers for Medicare & Medicaid Services
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPI	Center for Program Integrity
DOE	Department of Energy
ERM	enterprise risk management
FAR	Federal Acquisition Regulation
FPS	Fraud Prevention System
Framework	GAO's Fraud Risk Management Framework
HHS	Department of Health and Human Services
IPERA	Improper Payments Elimination and Recovery Act of 2010
IPERIA	Improper Payments Elimination and Recovery Improvement Act of 2012
IPIA	Improper Payments Information Act of 2002
IRS	Internal Revenue Service
LIHEAP	Low-Income Home Energy Assistance Program
OECD	Organisation for Economic Co-operation and Development
OIG	Office of Inspector General
OMB	Office of Management and Budget
SSA	Social Security Administration
SSN	Social Security number

Foreword

I am pleased to present GAO's Fraud Risk Management Framework (the Framework). The Framework includes a comprehensive set of leading practices that serve as a guide for program managers to use when developing or enhancing efforts to combat fraud in a strategic, risk-based manner. As the steward of taxpayer dollars, federal managers have the ultimate responsibility in overseeing how hundreds of billions of dollars are spent annually. Thus, they are well positioned to use these practices, while considering the related fraud risks as well as the associated benefits and costs of implementing the practices, to help ensure that taxpayer resources are spent efficiently and effectively.

The revised *Standards for Internal Control in the Federal Government* requires managers to assess fraud risks as part of their internal control activities. These standards become effective at the start of fiscal year 2016. The Framework provides comprehensive guidance for conducting these assessments and using the results as part of the development of a robust antifraud strategy. It also describes leading practices for establishing an organizational structure and culture that are conducive to fraud risk management, designing and implementing controls to prevent and detect potential fraud, and monitoring and evaluating to provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud.

The Framework has gone through a deliberative process, and a wide range of views were solicited in developing leading practices and ensuring their applicability to the federal government. This process included interactions with selected federal agency program officials, Offices of Inspector General, the World Bank, the Organisation for Economic Co-operation and Development, as well as antifraud experts from state and local governments, private companies, other national audit institutions, and nongovernmental organizations. The views of all parties were thoroughly considered in finalizing this document. I extend special thanks to those who commented and suggested improvements to the Framework.

Stephen M. Lord
Managing Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
July 2015

Introduction

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

Effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded.[1] Legislation and guidance issued since 2002 has focused managers' attention on addressing improper payments, which includes payments made as a result of fraud.[2] However, the deceptive nature of fraud makes it difficult to measure in a reliable way, and federal managers face fraud risks beyond those captured by improper payments, such as risks that do not pose a direct financial cost to taxpayers. For example, passport fraud poses a risk, because fraudulently-obtained passports can be used to conceal the true identity of the user and potentially facilitate other crimes, such as international terrorism and drug trafficking.[3]

Managers of government programs maintain the primary responsibility for enhancing program integrity; however, the Office of Management and Budget (OMB) plays a key role in issuing guidance to assist managers with combating government-wide fraud, waste, and abuse. OMB has established guidance for federal agencies on reporting, reducing, and recovering improper payments, including Appendix C to Circular A-123.[4] Moreover, legislation and guidance has increasingly focused on the need for program managers to take a strategic approach to managing risks, including fraud. For example, in 2014, OMB recommended that agencies consider adopting enterprise-wide risk management, an approach for addressing the full spectrum of risks and challenges related to achieving the agencies' missions.[5]

Our body of work has shown that managers have taken positive steps to address improper payments, but work remains to improve the integrity of government programs.[6] In particular, our work has shown that opportunities exist for federal managers to take a more strategic, risk-based approach to managing fraud risks and developing effective antifraud controls. For example, we reported in November 2014 on fraud related to disability benefit claims, concluding that the agency responsible for the program launched initiatives to combat fraud, but lack of planning, data, and coordination hampered the success of its efforts.[7] We also found in December 2014 that, to comply with legislation on improper payments, one agency developed a process to assess improper-payment risks, but its 2011 risk assessments did not fully evaluate risks and the agency did not always include a clear basis for risk determinations.[8] In addition, our reports on high-risk areas in the federal government have consistently highlighted programs' efforts to manage fraud, waste, and abuse.[9] To focus managers' attention on the need to take a more strategic, risk-based approach to managing fraud risks, the *Standards for Internal Control in the Federal Government*, commonly known as the Green Book, and hereafter referred to as *Federal Internal Control Standards*, requires managers to consider the potential for fraud when identifying, analyzing, and responding to risks.[10]

Implementing a risk-based approach to addressing potential fraud in the federal government poses a unique set of challenges to federal managers, given their programs'

mission to provide the public with a broad range of critical, often time-sensitive, services and financial assistance. Managers may perceive a conflict between their priorities to fulfill the program's mission, such as efficiently disbursing funds or providing services to beneficiaries, and taking actions to safeguard taxpayer dollars from improper use. However, the purpose of proactively managing fraud risks is to facilitate, not hinder, the 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 concepts and leading practices to aid federal program managers in managing fraud risks. We organized these concepts and practices into a Fraud Risk Management Framework (the Framework). The leading practices described in the Framework are meant to provide additional guidance for implementing requirements contained in *Federal Internal Control Standards*, improper-payment legislation, and OMB circulars.[11] In developing the Framework, we considered the fact that fraud can take many forms across the federal government, some programs are more vulnerable to fraud than others, and expertise to combat fraud varies within programs. Managers are responsible for determining the extent to which the leading practices presented in the Framework are relevant to their program and for tailoring the practices, as appropriate, to align with the program's operations. In doing so, managers consider applicable laws and regulations, the specific risks the program faces, and the associated benefits and costs of implementing each practice. While the primary target audience of this study is managers in the U.S. federal government, the practices and concepts described in the Framework may also be applicable to state, local, and foreign government agencies, as well as nonprofit entities that are responsible for fraud risk management.

To address our objective, we gathered testimonial evidence from multiple sources, including officials from Offices of Inspector General (OIG) for eight U.S. federal agencies, the Council of the Inspectors General for Integrity and Efficiency, and the national audit offices of three other countries.[12] Specifically, we interviewed officials from the OIGs of the five largest federal agencies by outlays and the five largest grant-making agencies, as well as officials from three national audit offices that have published reports related to our objective.[13] In addition, we interviewed antifraud experts from 10 other external entities, which we identified through our background research and discussions with internal fraud experts. We selected entities that represent different sectors, including private companies, state and local audit associations, nonprofit organizations, and intergovernmental organizations. The entities we selected also had expertise in different areas related to fraud risk management, such as audits, investigations, trainings, the design and implementation of fraud controls, and developing integrity frameworks.

Further, we attended a prominent antifraud conference and conducted three focus groups of 7 to 10 fraud risk management experts during the conference. Two focus groups consisted of fraud risk management experts that presented at the conference, and one focus group involved conference participants with relevant antifraud experience or knowledge. We also conducted an extensive literature review, a review of GAO's past work on fraud, internal controls, and program integrity, as well as additional reading that was recommended in our interviews and by internal experts. As part of our research, we considered existing frameworks and guides related to fraud risk management and integrity, including publications by the Australian National Audit Office, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the Organisation for Economic Co-operation and Development (OECD), as well as the Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners (ACFE), among others.[14]

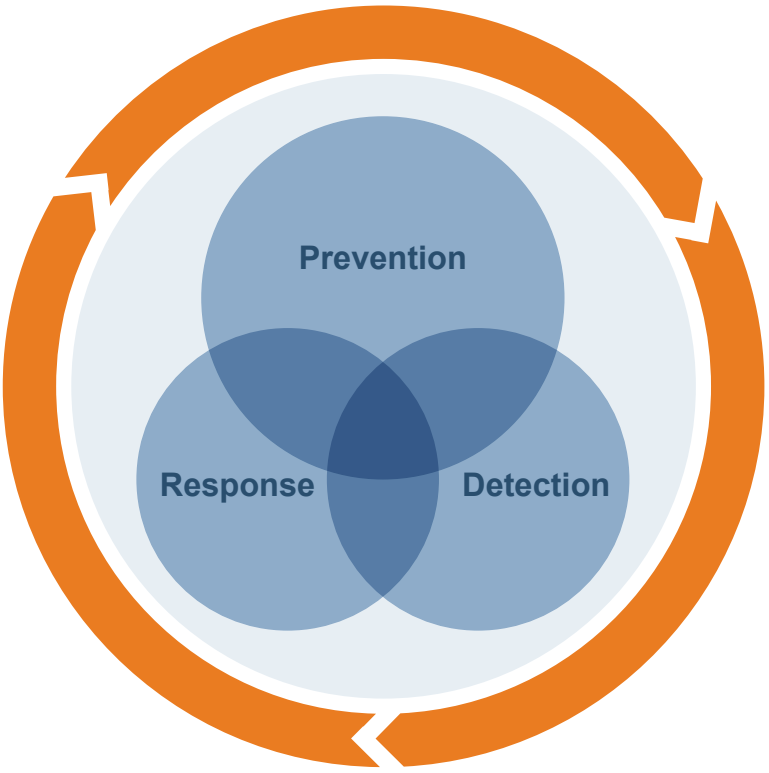
To validate our leading practices, we asked program officials associated with the same agency as the OIGs we interviewed to review the leading practices in a draft of the Framework. Moreover, to gain an additional perspective of a smaller agency than those we selected above, we asked a program within an agency with one of the lowest amount of outlays for fiscal year 2013 to review the leading practices. We incorporated input we received from programs into our study, as appropriate. In addition to the comments we sought for independent validation of leading practices, we provided a draft of the Framework to selected officials and experts who participated in our interviews to confirm that we captured their comments accurately and completely (see app. I for a detailed discussion of our methodology).

We conducted our work from March 2014 to July 2015 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objective. This framework requires that we plan and perform our work to obtain sufficient and appropriate evidence to meet our stated objective and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any conclusions in this product.

The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and impact of fraud.[15] As indicated above, this objective is meant to facilitate achievement of the program's broader mission and strategic goals by helping to ensure that funds are spent effectively, services fulfill their intended purpose, and assets are safeguarded.[16] The critical control activities for managing fraud risks fall into three general categories—prevention, detection, and response. These categories are interdependent and mutually reinforcing. For instance, detection activities, like surprise audits, also serve as deterrents because they create the perception of controls and possibility of punishment to discourage fraudulent behavior. In addition, response efforts can inform preventive activities, such as using the results of investigations to enhance applicant screenings and fraud indicators.

As depicted by the larger circle for prevention in figure 1, preventive activities generally offer the most cost-efficient use of resources, since they enable managers to avoid a costly and inefficient "pay-and-chase" model.[17] Therefore, leading practices for strategically managing fraud risks emphasize risk-based preventive activities, as discussed further in subsequent sections.

Figure 1: Interdependent and Mutually Reinforcing Categories of Fraud Control Activities



Source: GAO. | GAO-15-593SP

The Framework encompasses the control activities described above, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks.[18] The Framework consists of the following four components for effectively managing fraud risks:

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

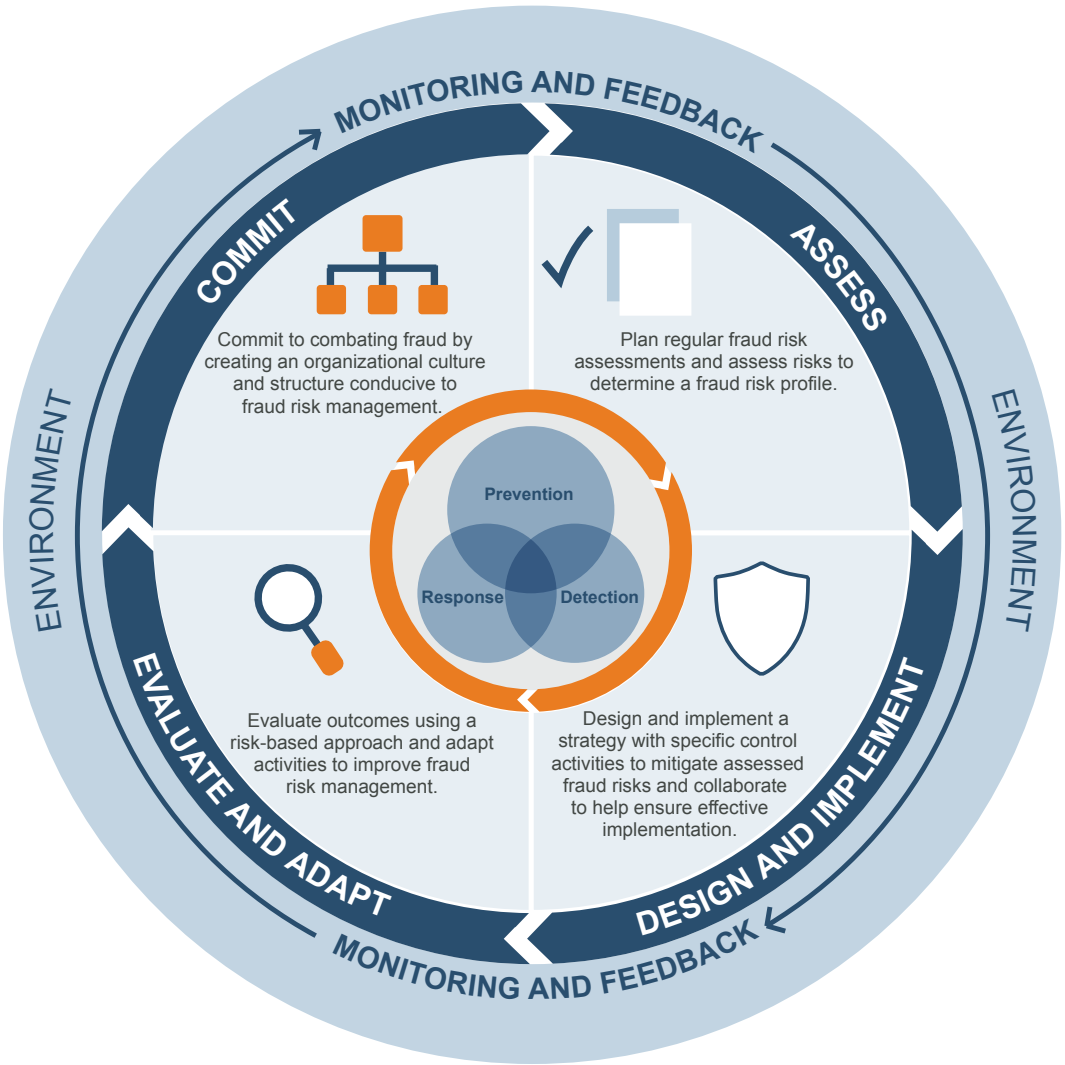
2. **Assess**—Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

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

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

In addition, the Framework reflects activities related to monitoring and feedback mechanisms, which include ongoing practices that apply to all four concepts above, as depicted in figure 2.

Figure 2: The Fraud Risk Management Framework



Source: GAO. | GAO-15-593SP

The "environment," as shown by the outer circle in figure 2, refers to contextual factors and stakeholders, either internal or external to an agency or program, which influence fraud risk management activities. For instance, an agency may have other initiatives to manage risks, such as enterprise-wide risk management efforts. Fraud risk management activities may be incorporated into or aligned with such internal activities and strategic objectives, to the extent they exist. Budgetary conditions can also affect a program's ability to pursue certain types of resource-intensive activities. In addition, activities of internal stakeholders, such as an OIG and its capacity to investigate potential fraud, can also influence and inform certain fraud risk management activities within a program.[19]

Other stakeholders and factors are external to a program and may also be beyond managers' direct control. These include other entities, such as contractors, different federal agencies, or state and local governments, as well as relevant laws, guidance, and standards, as described above, which may also affect managers' ability to implement specific activities.[20] For instance, participants of a forum we hosted in January 2013 about data analytics discussed legal constraints they said can hinder agencies' ability to use data to detect fraud, such as steps the Computer Matching Act requires of agencies before they can use data for matching purposes.[21]

A Guide for Reading the Framework

As a result of contextual differences between programs, the approach managers use to implement the leading practices described in the Framework may also vary. For example, some programs may already have certain control activities in place as part of existing risk management efforts. The leading practices in the Framework can be modified to fit the circumstances and conditions that are relevant to each program. Moreover, the practices in the Framework are not necessarily meant to be sequential or interpreted as a step-by-step process, unless indicated otherwise.

All subheaders (e.g., 1.1 and 1.2) in the sections below refer to overarching concepts of fraud risk management. Below each subheader we discuss leading practices that demonstrate ways for program managers to carry out the overarching concepts of the Framework. The overarching concepts and leading practices are summarized in a table at the beginning of each section, as follows:

Overarching Concepts
Leading Practices

Any use of the term "should" or "requires" denotes a standard or requirement described in improper-payment legislation, OMB guidance, or principles in *Federal Internal Control Standards*. We use terms like "may" or "should consider" when referring to attributes in *Federal Internal Control Standards*, which are characteristics that explain principles in further detail, but are not requirements for managers. To the extent they are relevant, we reference these sources in the endnotes (see app. VI); links to relevant laws, guidance, and standards may not be exhaustive.

1 Commit to Combating Fraud by Creating an Organizational Culture and Structure Conducive to Fraud Risk Management

Table 1: Leading Practices for Creating a Culture and Structure to Manage Fraud Risks

1.1 Create an Organizational Culture to Combat Fraud at All Levels of the Agency
Demonstrate a senior-level commitment to integrity and combating fraud.
Involve all levels of the agency in setting an antifraud tone that permeates the organizational culture.
1.2 Create a Structure with a Dedicated Entity to Lead Fraud Risk Management Activities
Designate an entity to design and oversee fraud risk management activities that • understands the program and its operations, as well as the fraud risks and controls throughout the program;[a] • has defined responsibilities and the necessary authority across the program; • has a direct reporting line to senior-level managers within the agency; and • is located within the agency and not the Office of Inspector General (OIG), so the latter can retain its independence to serve its oversight role.
In carrying out its role, the antifraud entity, among other things • serves as the repository of knowledge on fraud risks and controls; • manages the fraud risk-assessment process; • leads or assists with trainings and other fraud-awareness activities; and • coordinates antifraud initiatives across the program.

Source: GAO. | GAO-15-593SP

[a]For the sake of consistency, we generally refer to programs throughout this study; however, the practices we discuss can apply to agencies as well. Managers decide whether to carry out each aspect of fraud risk management at the program level or agency level.

1.1 Create an Organizational Culture to Combat Fraud at All Levels of the Agency

Managers who effectively manage fraud risks demonstrate a senior-level commitment to integrity and combating fraud.[22] Various actions can help managers meet this leading practice. For instance, according to experts we interviewed and literature we reviewed, managers can demonstrate their commitment to combating fraud and promoting integrity by conducting self-assessments of their performance in managing fraud risks, or establishing a code of conduct that sets expectations for ethical behavior, integrity standards for new hires, and an attitude statement towards fraud. Moreover, as discussed in detail below, managers who effectively manage fraud risks develop, document, and communicate an antifraud strategy that describes the program's approach to combating fraud. Effective fraud risk managers also involve all levels of the agency, such as mid-level managers and entry-level employees, in setting an antifraud tone that permeates the organizational culture. According to officials of one agency we interviewed, there needs to be "horizontal pressure" among peers within an agency to encourage fraud risk management, not just "vertical pressure." The text box below provides an example of an agency that has demonstrated senior-level commitment and established a dedicated antifraud entity to combat fraud, waste, and abuse, as discussed in the next section.

GAO's High-Risk Series and the Centers for Medicare & Medicaid Services (CMS)

We use five criteria when reviewing steps taken in high-risk areas,[a] one of which is "leadership commitment."[b] CMS has met our criterion for demonstrating strong commitment to—and top leadership support for—reducing the incidence of improper payments in the Medicare program. The Department of Health and Human Services (HHS) has continued to designate "strengthened program integrity through improper payment reduction and fighting fraud" as a department strategic priority. Through its dedicated Center for Program Integrity, which is CMS's focal point for all national Medicare program-integrity issues, CMS has taken multiple actions to improve in this area. For instance, CMS centralized the development and implementation of automated edits—prepayment controls used to deny Medicare claims that should not be paid. We reported in February 2015 that while CMS has met the criterion for leadership commitment, and has partially met each of the other criteria for removing Medicare improper payments from the High-Risk List, additional actions are needed to address fraud, waste, and abuse.[c] For instance, we reported that CMS could address the identity theft risks associated with having Social Security numbers on Medicare beneficiaries' health-insurance cards. Having senior-level commitment and a dedicated antifraud entity, as exemplified by CMS, are fundamental aspects of the Framework. However, other components and leading practices discussed in subsequent sections are also critical for effectively managing fraud risks.

---

[a]Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation. We designated Medicare as a high-risk program in 1990 due to its size, complexity, and susceptibility to mismanagement and improper payments. CMS, which administers Medicare for HHS, is responsible for overseeing the program and safeguarding it from loss.

[b]The other criteria include capacity, an action plan, monitoring, and demonstrated progress. See www.gao.gov for additional information on our high-risk series.

[c]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

1.2 Create a Structure with a Dedicated Entity to Lead Fraud Risk Management Activities

Federal Internal Control Standards requires managers to establish an organizational structure, among other actions, to achieve the program's objectives.[23] A leading practice for managing fraud risks is to designate an entity within that structure to design and oversee fraud risk management activities.[24] The dedicated entity could be an individual or a team, depending on the needs of the agency. For purposes of this study, we refer to this individual or team as the "antifraud entity." In addition to the antifraud entity, employees across an agency or program, as well as external entities, can be responsible for the actual implementation of fraud controls. Moreover, *Federal Internal Control Standards* requires managers to hold employees and external entities accountable for their internal control duties, which include activities for managing fraud risks.[25]

We identified the following leading practices to help managers decide who to assign as the antifraud entity. The antifraud entity

- understands the program and its operations, as well as the fraud risks and controls throughout the program;
- has defined responsibilities and the necessary authority across the program; and
- has a direct reporting line to senior-level managers within the agency.

In addition, it is critical that the antifraud entity be located within the agency and not the OIG, so the OIG can retain independence to serve its oversight role.[26] The specific department or unit that serves as the antifraud entity may vary, depending on factors like the existing structure or expertise within an agency. For instance, officials of one agency said the Office of General Counsel is best-suited to serve as the antifraud entity, given the agency's particular set of circumstances. Among other reasons, officials noted having the Office of General Counsel as the lead on combating fraud helps to alleviate perceived conflicts of interest that program managers may have between serving the agency's mission and managing fraud risks. In addition, agencies may have existing departments that are responsible for enterprise-wide risk management or managing risks related to improper payments. These departments may have functions that overlap with fraud risk management activities and they may be able to incorporate the roles and responsibilities of the antifraud entity. While the placement of an antifraud entity can vary by agency, the leading practices noted above for assigning the entity can aid managers in making this determination in any context.

As noted, the antifraud entity designs and oversees fraud risk management activities. Additional leading practices related to the antifraud entity's responsibilities include the following:

- serves as the repository of knowledge on fraud risks and controls,
- manages the fraud risk assessment process, and
- leads or assists with trainings and other fraud-awareness activities.

Other responsibilities may vary by program; however, the entity is generally responsible for coordinating antifraud initiatives across the program, such as facilitating communication with management and among stakeholders on fraud-related issues.[27] For instance, the Center for Program Integrity at CMS, the antifraud entity noted in the text box above, was designed to oversee all of CMS interactions and coordinate with key stakeholders related to program integrity (e.g., the Department of Justice, the OIG, and state law-enforcement agencies) for purposes of combating fraud and abuse.[28]

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

2.1 Plan Regular Fraud Risk Assessments That Are Tailored to the Program

Federal Internal Control Standards requires managers to assess fraud risks and consider the potential for internal and external fraud when identifying, analyzing, and responding to risks.[29] As noted, a leading practice in fraud risk management is for managers to dedicate an entity to manage this process. An effective antifraud entity tailors the approach for carrying out fraud risk assessments to the program. Factors such as size, resources, maturity of the agency or program, and experience in managing risks can influence how the entity plans the fraud risk assessment. For instance, an agency may have enterprise-wide or other risk management activities, such as processes to assess risks that affect operations or compliance with laws. These activities can inform the specific approach taken for assessing fraud risks. In addition, a program may have experienced a recent structural change, or added new services, which could necessitate more-frequent risk assessments.[30]

The factors noted above may also affect the frequency with which antifraud entities update the fraud risk assessment. In general, allowing extended periods of time to pass between fraud risk assessments could result in control activities that do not effectively address the program's risks. According to experts we interviewed, the frequency of updates can range from 1 to 5 years, and one company suggested quarterly reviews of the assessment. While the timing can vary, effective antifraud entities plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as fraud risk assessments are iterative and not meant to be onetime exercises. In commenting on a draft of the Framework, officials representing a task force sponsored by COSO and ACFE said the frequency of fraud risk assessments is a function of need and not just a matter of demonstrating compliance with standards.

Antifraud entities that effectively plan fraud risk assessments identify specific tools, methods, and sources for gathering information about fraud risks. This includes data on fraud schemes and trends from monitoring and detection activities. For instance, programs may develop surveys, or add questions to existing surveys that specifically address fraud risks and related control activities. In some programs, it may be possible to conduct focus groups or review documentation from reporting mechanisms, such as hotline reports and referrals, to identify fraud risks affecting the program. In addition, antifraud entities may engage relevant stakeholders in one-on-one interviews or brainstorming sessions about the types of fraud risks. A leading practice for involving stakeholders in this process is to include individuals responsible for the design and implementation of the program's fraud controls. This could include a variety of internal and external stakeholders, such as general counsel, contractors, or other external entities with knowledge about emerging fraud risks or responsibilities for specific control activities. In addition, the OIG and its work may inform the fraud risk assessment process and help managers to identify fraud risks. However, the OIG itself, as indicated in *Federal Internal Control Standards*, should not lead or facilitate the fraud risk assessments, in order to preserve its independence when reviewing the program's activities.[31]

2.2 Identify and Assess Risks to Determine the Program's Fraud Risk Profile

Managers who effectively assess fraud risks attempt to fully consider the specific fraud risks the agency or program faces, analyze the potential likelihood and impact of fraud schemes, and then ultimately document prioritized fraud risks. Moreover, managers can use the fraud risk assessment process to determine the extent to which controls may no longer be relevant or cost-effective.[32] There is no universally accepted approach for conducting fraud risk assessments, since circumstances between programs vary; however, assessing fraud risks generally involves the following five actions:[33]

1. Identify inherent fraud risks affecting the program:[34] Using methodologies discussed above, managers determine

where fraud can occur and the types of internal and external fraud risks the program faces, such as fraud related to financial reporting, misappropriation of assets, corruption, and nonfinancial forms of fraud.[35] These broad categories of fraud encompass specific fraudulent schemes related to contracting, grant-making, beneficiary payments, payroll payments, and other areas of government activity. Further, according to *Federal Internal Control Standards*, managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.[36]

2. Assess the likelihood and impact of inherent fraud risks: Managers may conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks on the program's objectives.[37] The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.[38] For instance, quantitative methodologies for analyzing the likelihood and impact of fraud involve statistical analysis, such as estimating the frequency of fraud and amount of losses based on a statistically valid sample or historical data of detected fraud. These quantitative techniques are generally more precise than qualitative methods, but they require resources and expertise to successfully implement, and may pose challenges for some managers, given the hidden nature of fraud (see app. II for further discussion on challenges of measuring fraud). Managers who effectively employ these techniques involve qualified specialists, such as statisticians and subject-matter experts, to provide expertise and guidance.

When resource constraints, available expertise, or other circumstances prohibit the use of statistical analysis for assessing fraud risks, other quantitative or qualitative techniques can still be informative.[39] For example, risk scoring quantifies the likelihood and impact of risks, and preferably uses an objective method in which the intervals between a score have meaning, such as using numeric rankings of 1 to 5 that indicate "rare" to "almost certain" for likelihood and "immaterial" to "extreme" for impact. These rankings can then be used to understand the overall significance of the risk on a similar five-point scale that represents, for instance, "very low" to "very high" (see fig. 3 later in this section for an illustration of this concept).

In addition to financial impacts, fraud risks can have an effect on the program's reputation and compliance with laws or regulations, and effective managers consider these nonfinancial impacts during the assessment process.[40] For example, managers may rank a particular type of fraud risk higher than other types of fraud if they perceive its impact on the program's reputation to be greater if it were to occur.

3. Determine fraud risk tolerance: According to *Federal Internal Control Standards*, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives.[41] 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.[42] Managers' defined risk tolerance may depend on the circumstances of individual programs and other objectives beyond mitigation of fraud risks. The following text box provides an illustrative example of risk tolerance applied to a program that provides disaster assistance.

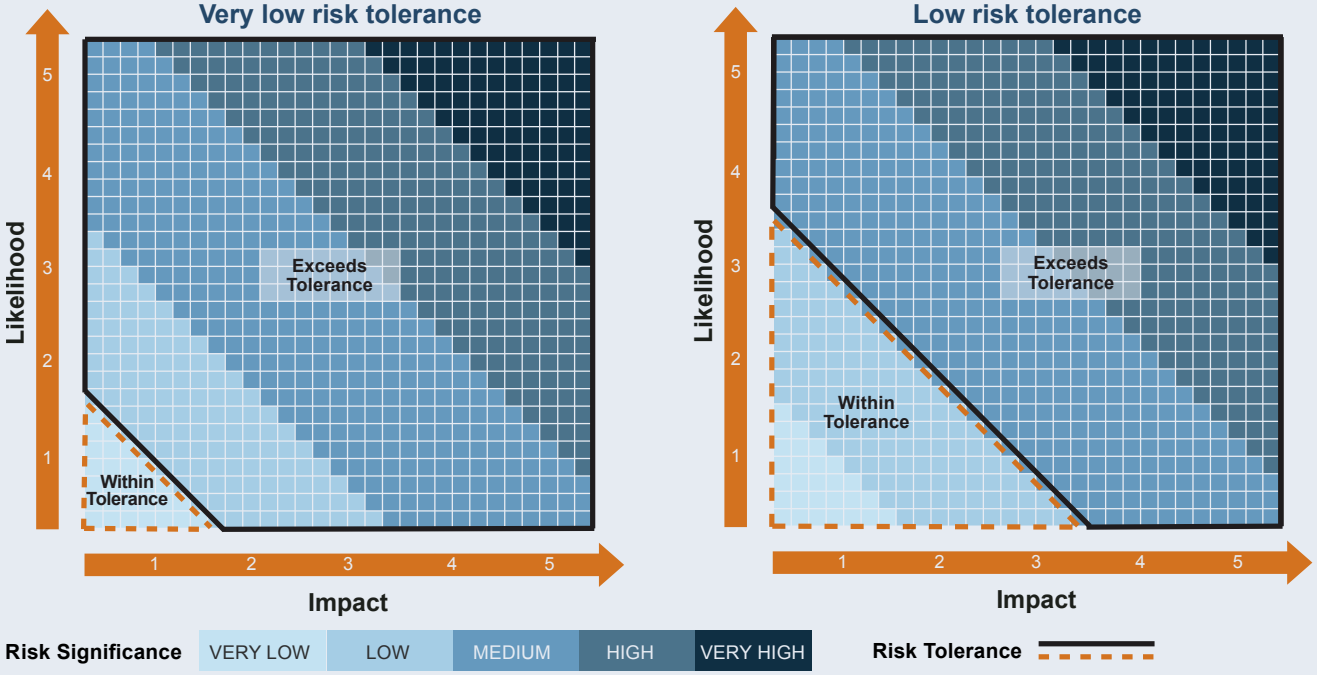
Example of Risk Tolerance and Risk Matrices in the Context of Natural Disaster Assistance

When responding to natural disasters, an assistance program has various control activities to prevent and detect fraudulent applications for its services, which include providing financial assistance for temporary housing to people whose homes were damaged or destroyed. Managers may generally define their risk tolerance as "very low" with regard to providing temporary housing assistance to potentially fraudulent applicants. Therefore, they require all applicants to undergo a home inspection to verify damage prior to the provision of any funds, since the inspections are a control activity that provides a high level of certainty that the assistance is actually going to those in need.

However, managers may have a higher fraud risk tolerance, such as "low" rather than "very low," for making payments to potentially fraudulent applicants if the individuals live in a severely damaged area, since individuals in these areas are likely to have an urgent need for temporary housing assistance. In such circumstances, managers may weigh the program's other operational objective of expeditiously providing assistance against the objective of lowering the likelihood of fraud, because activities to lower the risk related to fraudulent applications, such as conducting inspections, may cause delays in service. Given a "low" fraud risk tolerance, as opposed to "very low," a manager may decide to postpone or forego home inspections, which may be time-consuming or difficult to conduct in inaccessible areas. Instead, the manager may allocate resources to a control activity with a lower level of certainty than inspections, such as using geospatial imagery to identify severely damaged areas and make eligibility determinations.

Figure 3 illustrates concepts described so far with a two-dimensional risk matrix, a common technique managers may employ to visually plot risks according to their likelihood and impact.[a] As noted, the specific methodology managers use to assess fraud risks can vary. This particular technique is useful for engaging individuals who are knowledgeable about a program, such as "front line" staff responsible for implementing control activities, and for helping managers understand the link between specific risks and their impact.[b] The first matrix illustrates a risk tolerance of "very low" and the second matrix shows a "low" risk tolerance, as discussed in the example above. See the "Design and Implement" section for further discussion on potential responses to fraud risks that either exceed or are within the risk tolerance.

Figure 3: Example of Two-Dimensional Risk Matrices



Source: GAO. | GAO-15-593SP

[a]When using this method, risks are mapped onto the matrix based on a ranked scale that generally indicates risks on a continuum of low to high risks. Risks that fall in the upper right quadrant are the most likely to occur and have the greatest consequences for the program, compared to risks that fall into the lower left quadrant. When risks are plotted together, managers can quickly determine which ones have top priority and better understand linkages between specific risks. As noted in *Federal Internal Control Standards*, managers may also consider correlations between risks, regardless of whether they choose to analyze risks on an individual basis or as categories of risks (see GAO-14-704G, 7.07).

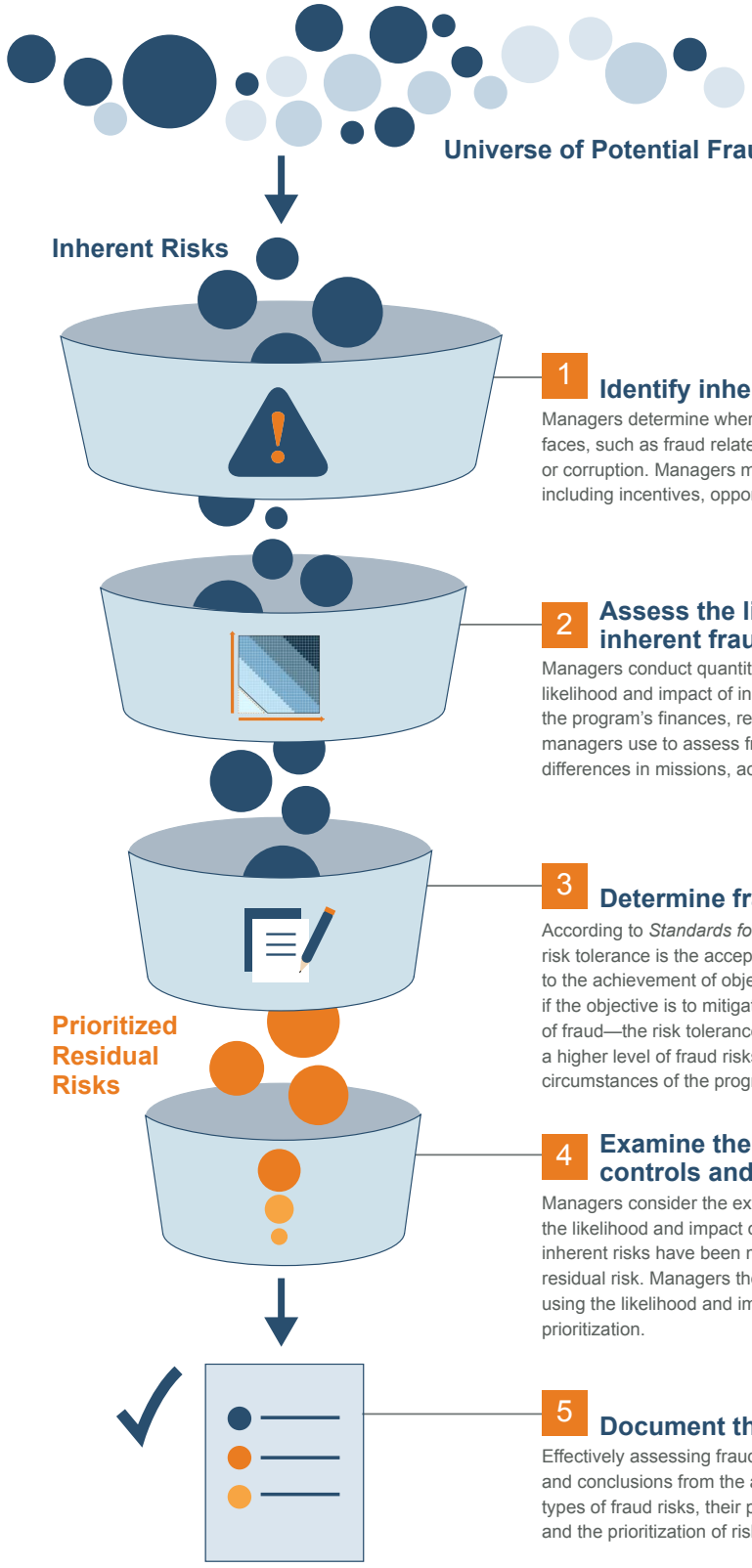
[b]A risk matrix and other approaches for assessing fraud risks, such as surveys, are based on perceptions and therefore they may not precisely reflect the actual likelihood or full impact of the fraud risks. Fraud risk assessments that involve relevant internal and external stakeholders are more likely to be successful and reflect a complete understanding of fraud risks and control vulnerabilities within an agency.

The text box above describes risk tolerance in qualitative terms; however, programs may also consider quantifying risk tolerances to the extent possible. For instance, a quantified risk tolerance could express managers' willingness to tolerate an estimated amount of potentially fraudulent activity, given resource constraints in eliminating all fraud risks. Regardless of the approach, managers should consider defining risk tolerances that are specific and measurable, as noted in *Federal Internal Control Standards*.[43] Moreover, according to our focus-group participants, eliminating fraud risk is not a realistic goal, and therefore effective managers define and document their level of tolerable fraud risk.

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 and whether the remaining risks exceed managers' tolerance.[44] The aforementioned actions for assessing risks focused on identifying and analyzing inherent fraud risks. At this stage, managers focus on connecting existing fraud risk management activities and controls to identified risks in order to further understand the likelihood and impact of the fraud risks affecting the program. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. This part of the fraud risk assessment process can help managers identify areas where existing control activities are not suitably designed or implemented to reduce risks to a tolerable level. Based on this analysis and defined risk tolerance, managers then rank residual fraud risks in order of priority, and determine their responses, if any, to mitigate the likelihood and impact of residual risks that exceed their risk tolerance (see the "Design and Implement" section). During this process, managers can also identify the responsible internal and external entities, or "owners," of the control activities that are meant to reduce fraud risks.

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 internal and external fraud risks, their perceived likelihood and impact, managers' risk tolerance, and the prioritization of risks. We refer to the summation of these findings as the program's "fraud risk profile" (see app. V for an example of a fraud risk profile). The fraud risk profile is an essential piece of an overall antifraud strategy and can inform the specific control activities managers design and implement, as described in the next section. Figure 4 summarizes the key elements of the fraud risk assessment process.

Figure 4: Key Elements of the Fraud Risk Assessment Process



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.

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.

3 Design and Implement a Strategy with Specific Control Activities to Mitigate Assessed Fraud Risks and Collaborate to Help Ensure Effective Implementation

Table 3: Leading Practices for Designing and Implementing an Antifraud Strategy with Control Activities

3.1 Determine Risk Responses and Document an Antifraud Strategy Based on the Fraud Risk Profile
Use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks.
Develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.
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.
Design and implement the following control activities to prevent and detect fraud:[a] • data-analytics activities, • fraud-awareness initiatives, • reporting mechanisms, and • employee-integrity activities.
3.3 Develop a Plan Outlining How the Program Will Respond to Identified Instances of Fraud
Develop a plan outlining how the program will respond to identified instances of fraud and ensure the response is prompt and consistently applied.
Refer instances of potential fraud to the OIG or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation.
3.4 Establish Collaborative Relationships with Stakeholders and Create Incentives to Help Ensure Effective Implementation of the Antifraud Strategy
Establish collaborative relationships with internal and external stakeholders, including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities to, among other things, • share information on fraud risks and emerging fraud schemes, and • share lessons learned related to fraud control activities.
Collaborate and communicate with the OIG to improve understanding of fraud risks and align efforts to address fraud.
Create incentives for employees to manage risks and report fraud, including • creating performance metrics that assess fraud risk management efforts and employee integrity, particularly for managers; and • balancing fraud-specific performance metrics with other metrics related to employees' duties.
Provide guidance and other support and create incentives to help external parties, including contractors, effectively carry out fraud risk management activities.

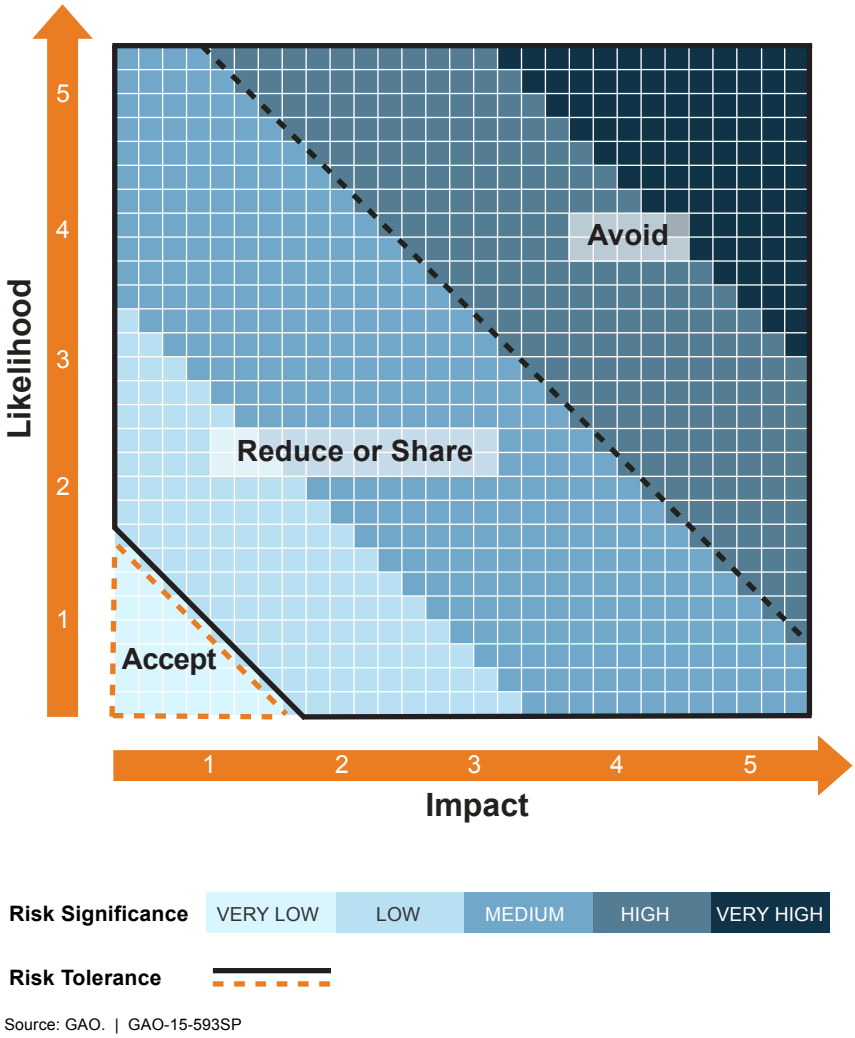
Source: GAO. | GAO-15-593SP

[a]See table 5 for additional leading practices related to each of these control activities.

3.1 Determine Risk Responses and Document an Antifraud Strategy Based on the Fraud Risk Profile

Federal Internal Control Standards requires managers to design a response to analyzed risks. Managers should consider the likelihood and impact of the risks, as well as their defined risk tolerance. These are key elements of a program's fraud risk profile, as previously discussed. Effective managers of fraud risks use the program's fraud risk profile to help decide how to allocate resources to respond to residual fraud risks.[45] The responses to fraud risks may include actions to accept, reduce, share, or avoid the risk.[46] In general, managers accept certain risks that are within their defined risk tolerance and take one of the other three actions in response to prioritized residual fraud risks that exceed their defined risk tolerance (see fig. 5). Specifically, managers may allocate resources to prevent or detect fraud risks that exceed their risk tolerance, but they may decide not to allocate resources to further reduce unlikely, low-impact risks that fall within their risk tolerance. Moreover, while managers may "accept" certain fraud risks, responding appropriately to instances of actual fraud is essential for ensuring the continued effectiveness of fraud risk management activities, as discussed later in this section.

Figure 5: Potential Responses to Fraud Risks Based on Assessed Likelihood, Impact, and Risk Tolerance



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.

3.2 Design and Implement Specific Control Activities to Prevent and Detect Fraud

As part of the antifraud strategy, managers who effectively manage fraud risks design and implement specific control activities—including policies, procedures, techniques, and mechanisms—to prevent and detect potential fraud. In addition to designing and implementing new control activities, managers may also revise existing control activities if they determine, as part of the fraud risk assessment process, that certain controls are not effectively designed or implemented to reduce the likelihood or impact of an inherent fraud risk to a tolerable risk level.

As discussed, while fraud control activities can be interdependent and mutually reinforcing, preventive activities generally offer the most cost-effective investment of resources. Therefore, effective managers of fraud risks focus their efforts on fraud prevention in order to avoid a costly "pay-and-chase" model, to the extent possible. In addition, automated control activities (e.g., automated data-analytic techniques) tend to be more reliable than manual control activities (e.g., document reviews) because they are less susceptible to human error and are typically more efficient. Further, experts from one private-sector organization we met with noted controls that are targeted to specific risks may be more expensive than agency-wide controls, such as requiring new employees to sign an antifraud policy. However, targeted controls may lower the cost of identifying each instance of fraud because they are more effective.

When developing an antifraud strategy, managers also consider the benefits and costs of control activities to address identified residual risks, such as the benefit to the program of reducing the likelihood or impact of a fraud risk and the direct financial cost of the control to the program. *Federal Internal Control Standards* states that managers may decide how to evaluate the benefits versus costs of various approaches to implementing an effective internal control system.[48] Approaches for considering the benefits and costs of control activities to address identified fraud risks include benefit-cost analysis and cost-effectiveness analysis.[49] The text box below provides additional information on using these approaches.

Approaches for Considering the Benefits and Costs of Fraud Control Activities

Benefit-cost analysis involves the systematic identification and monetization of all benefits and costs associated with designing and implementing a control activity, as well as how those benefits and costs are distributed across different groups. Based on a benefit-cost analysis, managers may decide not to implement certain control activities for which the estimated benefits do not exceed the costs. For example, managers may decide not to conduct payment-recapture audits to recover improper payments if it is likely that the costs incurred to identify and recover the overpayments will be greater than the expected recoveries.[a] While benefit-cost analysis can help managers determine whether benefits of a control activity exceed its costs, managers may face challenges in monetizing certain benefits and costs.[b] For example, in addition to direct financial benefits and costs to the program, fraud controls may result in additional benefits, such as the value of deterred fraud, or other costs, such as delays for legitimate applicants. In such circumstances, cost-effectiveness analysis—a methodology for determining the cost to achieve a particular objective, expressed in nonmonetary terms—can be appropriate.

Managers may consider cost-effectiveness analysis when the benefits from competing alternatives are the same or where a law or policy requires a program to achieve a particular objective.[c] For instance, if a program's policies require verification that applicants provide a valid address in order to enroll in a program or receive benefits, managers may use cost-effectiveness analysis to compare alternative means of achieving this objective. In this example, the analysis could weigh two alternatives, such as using federal government databases to electronically verify addresses and paying inspectors to physically verify each address, in order to determine the option with the lowest cost per invalid address identified. As illustrated by this example, cost-effectiveness analysis enables managers to assess alternatives without having to calculate the monetary value of the benefits of each option.

---

[a]However, OMB requires an agency that determines that it would be unable to conduct a cost-effective payment-recapture audit program for certain programs that expend more than $1 million to notify OMB and the agency's Inspector General of this decision and include any analysis used by the agency to reach this decision. OMB may review these materials and determine that the agency should conduct a payment-recapture audit to review these programs and activities. Office of Management and Budget, *Requirements for Effective Estimation and Remediation of Improper Payments*, Circular No. A-123, app. C (Washington, D.C.: 2014).

[b]See app. II for further discussion of the challenges related to measuring fraud.

[c]OMB guidelines state that benefit-cost analysis is the preferred methodology for analyzing government programs, but note that cost-effectiveness analysis can be appropriate in these circumstances. In addition, the guidelines note that a comprehensive enumeration of the different types of benefits and costs can be helpful in identifying the full range of program effects and can provide useful insights even when the monetary values of some benefits or costs cannot be determined. Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Circular No. A-94, Revised (Washington, D.C.: Oct. 29, 1992).

In addition to benefit-cost and cost-effectiveness analyses, internal and external environmental factors, such as legal requirements or budgetary conditions, may inform managers' decisions about the appropriateness of certain control activities for a particular program. These environmental factors, as well as the types of risks programs face, can contribute to variation in control activities used by different programs.[50] For example, in comments on a draft of this study, officials from one federal agency noted the agency's OIG identified instances of fraud perpetrated by external parties that were responsible for aspects of a program's operations. However, according to agency officials, the agency does not have statutory authority to collect certain information from these external parties, such as Social Security numbers (SSN), and therefore the agency is limited in its ability to use data analytics to detect fraud by these parties (see below for further discussion on data analytics). This may not be a factor for managers of other programs, such as those who manage programs that do not rely on external parties for operations. While statutory limitations and other environmental factors beyond the direct control of managers may affect the extent to which certain control activities are appropriate and feasible for a program, *Federal Internal Control Standards* nonetheless requires managers to design control activities to respond to risks, including fraud risks.[51] Therefore, managers of programs with environmental factors that limit the use of certain control activities discussed below may need to identify alternatives for effectively responding to identified fraud risks.

Given the scope of this study, we do not provide an exhaustive list of all control activities that a program may need to address every fraud scheme or manage all risks they may face in specific contexts.[52] In addition, we do not address in detail certain control activities that are required by existing legislation, guidance, or standards. For example, when assigning roles and responsibilities for certain control activities, *Federal Internal Control Standards* says managers should consider segregation of duties. This control helps to prevent fraud by separating activities related to authority, custody, and accounting and can help address the risk of management override, which circumvents existing control activities and increases fraud risks.[53] Nevertheless, certain control activities are broadly applicable to programs. For purposes of this study, we focus on the following types of control activities:

- data-analytics activities,
- fraud-awareness initiatives,
- reporting mechanisms, and
- employee-integrity activities.

Environmental and contextual factors specific to the program, such as those that may inform managers' determinations about the appropriateness of control activities, can also influence the precise way managers design and implement each of these four activities. For example, some control activities may already exist as part of an agency's other risk management initiatives. In such circumstances, managers may revise existing activities to help ensure they are designed and implemented to effectively address fraud risks in particular. Moreover, while the antifraud entity is generally responsible for designing and overseeing fraud risk management efforts, other individuals or offices, including external parties, may be responsible for designing or implementing certain activities. For instance, the OIG may operate a hotline for the agency, or the agency may rely on the Office of Personnel Management to conduct background investigations to identify integrity issues that may affect applicants' suitability for employment with the federal government.

As noted in table 3 at the beginning of this section, in general, it is a leading practice for managers to have efforts related to all four control activities to help with fraud risk management. We identified additional leading practices that expand on the design and implementation of each of these activities, summarized in table 5. In addition, we provide further information on leading practices and considerations related to data-analytics activities and fraud-awareness initiatives in appendix III.

Table 5: Additional Leading Practices for Data-Analytics Activities, Fraud-Awareness Initiatives, Reporting Mechanisms, and Employee-Integrity Activities

Data-Analytics Activities[a] Data-analytics activities can include a variety of techniques. For example, data mining and data-matching techniques can enable programs to identify potential fraud or improper payments that have already been awarded, thus assisting programs in recovering these dollars, while predictive analytics can identify potential fraud before making payments.[b]	Take a risk-based approach to data analytics and consider the benefits and costs of investing in specific data-analytic tools and techniques.
	Build support within the program for data-analytics activities.
	Ensure employees have sufficient knowledge, skills, and training to perform data analytics.
	Combine data across programs and from separate databases within the agency to facilitate reporting and analytics, if legally permissible.
	Pursue access to necessary external data, including pursuing data-sharing agreements.
	Consider program rules and known or previously encountered fraud schemes to design data-analytic tests.
	Conduct the following data-analytics activities to prevent and detect fraud: • Apply system edit checks to help ensure data meet requirements before data are accepted into the program's system and before payments are made. • Conduct data matching to verify key information, including self-reported data and information necessary to determine eligibility. • Conduct data mining to identify suspicious activity or transactions, including anomalies, outliers, and other red flags in the data.
	Automate data-analytic tests to monitor data for fraud indicators on a continuous, real-time basis.
	Tailor the output of data analytics to the intended audience to help ensure the results are usable.
	Review the results of data analytics and refer appropriate cases to the Office of Inspector General (OIG) for further investigation.
Fraud-Awareness Initiatives[a] Increasing managers' and employees' awareness of potential fraud schemes through training and education can serve a preventive purpose by helping to create a culture of integrity and compliance within the program. Further, increasing fraud awareness can enable managers and employees to better detect potential fraud. In addition, increasing fraud awareness externally can help prevent and deter fraud.	Require all employees, including managers, to attend training upon hiring and on an ongoing basis thereafter, and maintain records to track compliance.
	Collaborate with the OIG when planning or conducting training and promote the results of successful OIG investigations internally.
	Provide training to stakeholders with responsibility for implementing aspects of the program, including contractors and other external entities responsible for fraud controls.
	Use multiple methods to reinforce key antifraud messages.
	Convey fraud-specific information that is tailored to the program and its fraud risk profile, including information on fraud risks, employees' responsibilities, and the effect of fraud.
	Take steps to increase awareness about program integrity and antifraud efforts outside the program, including publicizing information on antifraud efforts and successfully resolved cases.

(continued on next page)

Reporting Mechanisms Reporting mechanisms include hotlines, whistleblower policies, and other mechanisms for receiving tips. Reporting mechanisms help managers to detect instances of potential fraud, and they can also deter individuals from engaging in fraudulent behavior if they believe that the fraud will be discovered and reported.	Provide multiple options in addition to hotlines for potential reporters of fraud to communicate, such as online systems, e-mail, fax, written formats, or face-to-face.
	Ensure individuals external to the agency that may be aware of potential fraud, such as vendors, program beneficiaries, and the public, can report potential fraud.
	Take steps to ensure individuals feel comfortable raising suspicions by providing them the opportunity to report suspicions anonymously if preferred, treating all reports confidentially, and establishing policies that prohibit retaliation for employees who make reports in good faith.
	Promote the existence of reporting mechanisms by reminding employees periodically about reporting mechanisms, and publicizing information on the reporting mechanism externally, such as including information about methods for reporting suspected fraud on the program's website.
Employee-Integrity Activities[c] Employee-integrity activities can prevent fraud by helping managers to establish a culture that is conducive to fraud risk management.	Take steps, such as conducting background checks, to screen employees for integrity issues, including prospective employees and employees in positions of trust or that pose a higher risk of fraud.
	Tailor the extent of employee screening to the risk level of the position.
	Develop and communicate a standard of conduct that applies to all employees and includes information on • the program's general expectations of behavior, using specific examples, such as cases of prohibited behavior and situations employees may encounter, and • the program's response to violations of the standard of conduct, such as disciplinary actions and sanctions.

Source: GAO. | GAO-15-593SP

[a]See app. III for additional information on designing and implementing data-analytics activities and fraud-awareness initiatives.

[b]Data matching is a process in which information from one source is compared with information from another, such as government or third-party databases, to identify any inconsistencies. Data mining analyzes data for relationships that have not previously been discovered. Predictive-analytics technologies include a variety of automated systems and tools that can be used to identify particular types of behavior, including potential fraud, before transactions are completed.

[c]Programs or agencies may already have certain employee-integrity activities in place to comply with existing requirements. For example, Executive Order 10450, as amended, requires all government agencies to establish and maintain a program to ensure that an applicant's employment is consistent with national security interests by, among other things, conducting checks to verify each applicant's past employment. In addition, *Federal Internal Control Standards* says managers should consider establishing standards of conduct to communicate expectations concerning integrity and ethical values (GAO-14-704G, 1.06–1.10). While these activities may be implemented by other offices within the agency, they are nevertheless important to a program's overall fraud risk management efforts.

3.3 Develop a Plan Outlining How the Program Will Respond to Identified Instances of Fraud

While preventive controls generally offer the most cost-effective investment of resources, managers who effectively manage fraud risks develop a plan that describes how the program will respond to instances of fraud that occur, despite existing controls. As with control activities to prevent and detect fraud, activities to respond to fraud are documented as part of the antifraud strategy, as noted in table 3. When instances of fraud are identified, managers take steps to ensure that they respond promptly and that the response is consistently applied.[54] Responding promptly and consistently to instances of fraud is critical for ensuring the continued effectiveness of fraud risk management activities. For example, a prompt and consistent response to instances of fraud identified through reporting mechanisms demonstrates that management takes reports seriously, which can incentivize future referrals. More broadly, the likelihood that individuals who engage in fraud will be identified and punished serves to deter others from engaging in fraudulent behavior. Further, responding appropriately to identified instances of fraud can remedy the harm caused by fraudulent actions and reduce the likelihood that offenders will be able to commit similar fraudulent acts in the future.

Effective managers of fraud risks refer instances of potential fraud to the OIG or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation. The specific actions a program should take in response to an act that has been determined to be fraudulent will depend on a variety of factors, including the type and severity of fraud and any legislative or regulatory requirements. Examples of response activities to actual fraud include disciplinary or administrative sanctions, such as suspensions, debarments, payment or loss recoveries, and fines, as well as legal actions, such as prosecutions.[55] Regardless of the specific actions taken, managers who effectively respond to identified fraud analyze data on instances of detected fraud and, if necessary, take corrective actions in response to that analysis, as discussed in more detail in the "Evaluate and Adapt" section.

3.4 Establish Collaborative Relationships with Stakeholders and Create Incentives to Help Ensure Effective Implementation of the Antifraud Strategy

When implementing control activities, effective managers of fraud risks establish collaborative relationships with internal and external stakeholders. More broadly, *Federal Internal Control Standards* requires managers to communicate quality information internally as well as with external parties.[56] Internal stakeholders include other offices within the agency, such as legal and ethics offices and offices responsible for other risk management activities, while external stakeholders can include other federal agencies, private-sector partners, state and local governments, law-enforcement entities, and contractors. In addition, external stakeholders may include others, such as recipients of federal funds. Managers who effectively manage fraud risks collaborate and communicate with these internal and external stakeholders to share information on fraud risks and emerging fraud schemes, as well as lessons learned related to fraud control activities. As discussed in the next section, information on fraud trends and lessons learned can be used to improve the design and implementation of fraud risk management activities. Managers can collaborate and communicate through a variety of means, including task forces, working groups, or communities of practice, as well as informally. The text box below illustrates one agency's effort to collaborate internally to enhance its management of fraud risks.

Example of Internal Collaboration to Enhance Fraud Risk Management

We reported in November 2012 about the Internal Revenue Service's effort to publish a report to consolidate and track information from multiple sources within the agency about identity-theft incidents, as well as efforts to combat fraud.[a] The report informs senior management and serves as a standard source of information for responding to data requests from external parties. Such reports are useful for program monitoring, providing management and other entities with up-to-date, consistent information about fraud schemes, and demonstrating the agency's response efforts. In addition, a report that draws from multiple sources within an agency can aid in communicating information about databases for combating fraud, including data limitations, sources, and the frequency of updates.

[a]GAO, *Identity Theft: Total Extent of Refund Fraud Using Stolen Identities is Unknown*, GAO-13-132T (Washington, D.C.: Nov. 29, 2012).

In addition, managers who effectively manage fraud risks collaborate and communicate with the OIG, if the agency has one, to improve their understanding of fraud risks. For instance, given the OIG's role in investigating instances of potential fraud, frequent communication with the OIG can help managers to identify emerging fraud risks and proactively enhance preventive activities. In addition, effective collaboration and communication with the OIG can help align efforts of key stakeholders to address potential fraud. For example, OIG officials of one agency told us a program manager may wish to suspend the disbursement of funds to individuals suspected of fraud, yet continued payments could aid law-enforcement entities in tracking the funds to build their case. According to these officials, open communication between the program offices, law-enforcement entities, and the OIG can help strike a balance between administrative and investigative efforts.

Further, effective managers of fraud risks create incentives for employees to contribute to fraud risk management and to report fraud. Incentives can vary. For example, OIG officials of one agency we interviewed said program offices within their agency recently began an initiative to recognize employees who work on antifraud issues. According to these officials, regions that had implemented the program were more active and productive in combating fraud. In addition, performance metrics that assess fraud risk management efforts and employee integrity can incentivize employees, including managers, to contribute to fraud risk management efforts. Managers who establish performance metrics related to fraud risk management and employee integrity balance these metrics with those that measure employees' performance related to other duties. As noted, individuals may perceive a conflict between effectively carrying out assigned tasks, such as disbursing funds quickly and implementing fraud controls to safeguard taxpayer dollars. Moreover, performance metrics for employees can perpetuate this conflict and create disincentives to combat fraud. For instance, we reported in November 2014 that one program's performance measures for its frontline employees responsible for processing applications for benefits focused on prompt processing, resulting in a disincentive for employees to report potential fraud because of the time it requires to develop a fraud referral.[57] Effective performance metrics reinforce the objectives of fraud risk management activities and strike a balance with other activities that serve the program's mission.

Finally, managers who effectively implement the antifraud strategy take steps to help ensure contractors and other external parties with responsibility over specific fraud control activities effectively implement those activities. The text box below provides additional discussion and leading practices related to collaborating with and incentivizing external parties to effectively manage fraud risks.

External Parties and Fraud Risk Management

Agencies routinely rely on external parties, such as other federal entities, state and local governments, and contractors, to implement aspects of the agencies' operations, including fraud control activities. For example, the Centers for Medicare & Medicaid Services (CMS) uses contractors to identify potential fraud, investigate it thoroughly and in a timely manner, and take swift action, such as working to revoke suspect providers' Medicare billing privileges and referring potentially fraudulent providers to law-enforcement entities. In addition, agencies with categorical eligibility policies rely on the effectiveness of external parties' fraud control processes to safeguard taxpayer dollars—an example of an external environmental factor that can influence a program's fraud risk management activities.[a] For instance, states may automatically enroll individuals in the Low-Income Home Energy Assistance Program (LIHEAP) based on the applicant or a household member receiving benefits from other federal programs, such as Temporary Assistance for Needy Families or the Supplemental Nutrition Assistance Program.[b] In such circumstances, a program's ability to mitigate fraud risks depends on the effectiveness of external parties' control activities to prevent and detect fraud.

Legislation, regulations, and OMB guidance require managers to take actions to oversee contractors and other external parties that are responsible for program operations. Moreover, *Federal Internal Control Standards* states that managers may engage external parties to perform certain processes for the program, but program managers retain responsibility for the performance of processes assigned to external parties.[c] Providing guidance and other support to external parties can help program managers to meet this standard. This could include sharing information on effective practices used by the program or other external parties, or providing opportunities for external parties to network and share information with each other about fraud risk management activities. In addition, effective managers of fraud risks create incentives for external parties, including contractors, to contribute to fraud risk management activities. For example, as with employees, incentives can be provided to contractors not just to process registrations and claims quickly, but also to prevent fraud. Throughout this study, we discuss leading practices for managers to involve external parties in other aspects of fraud risk management, such as including them in processes to assess fraud risks or providing them with fraud-awareness training.

---

[a]In general, categorical eligibility is a policy whereby an individual receives automatic or "categorical" eligibility for one program based on eligibility for or receiving benefits from another program. The intent of categorical eligibility is to increase program access and reduce the administrative burden on state agencies by streamlining the need to apply means tests.

[b]LIHEAP grantees may also set additional LIHEAP eligibility criteria, such as passing an assets test; living in nonsubsidized housing; having a household member who is elderly, disabled, or a young child; or having received a utility disconnection notice. We reported in June 2010 that the effectiveness of LIHEAP's preventive controls depended on the effectiveness of the preventive controls for the federal program from which the recipient originally received benefits. We recommended that the Department of Health and Human Services (HHS) consider issuing guidance to the states to evaluate the feasibility of using third-party sources to provide assurance that individuals do not exceed maximum income thresholds. HHS addressed our recommendation by issuing a memorandum in May 2010 encouraging states to access state directories of new hires or similar systems to confirm income eligibility. See GAO, *Low-Income Home Energy Assistance Program: Greater Fraud Prevention Controls Are Needed*, GAO-10-621 (Washington, D.C.: June 18, 2010).

[c]GAO-14-704G, OV4.01–4.03. Management may consider the following when determining the extent of oversight for the operational processes assigned to the service organization: the nature of services outsourced; the service organization's standards of conduct; the quality and frequency of the service organization's enforcement of adherence to standards of conduct by its personnel; the magnitude and level of complexity of the entity's operations and organizational structure; the extent to which the entity's internal controls are sufficient so that the entity achieves its objectives and addresses risks related to the assigned operational process.

4 Evaluate Outcomes Using a Risk-Based Approach and Adapt Activities to Improve Fraud Risk Management

Table 6: Leading Practices for Monitoring, Evaluating, and Adapting Fraud Risk Management Activities

4.1 Conduct Risk-Based Monitoring and Evaluate All Components of the Fraud Risk Management Framework
Monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts.
Collect and analyze data, including data from reporting mechanisms and instances of detected fraud, for real-time monitoring of fraud trends and identification of potential control deficiencies.
Employ a risk-based approach to monitoring by taking into account internal and external factors that can influence the control environment, such as organizational changes and emerging risks.
In the absence of sufficient data, assess how well managers follow recommended “leading practices” for designing fraud risk management activities.
4.3 Adapt Fraud Risk Management Activities and Communicate the Results of Monitoring and Evaluations
Use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities.
Use analysis of identified instances of fraud and fraud trends to improve fraud risk management activities, including prioritizing and taking corrective actions, as well as enhancing fraud-awareness trainings.
Use results of investigations and prosecutions to enhance fraud prevention and detection.
Communicate results of monitoring and evaluations, including corrective actions taken, if any, to relevant stakeholders.

Source: GAO. | GAO-15-593SP

4.1 Conduct Risk-Based Monitoring and Evaluate All Components of the Fraud Risk Management Framework

Ongoing monitoring and periodic evaluations provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud. Monitoring and evaluation activities can also support managers' decisions about allocating resources, and help them to demonstrate their commitment to effectively managing fraud risks. Effective managers assess activities related to all components of the Framework, and not just control activities built into operational processes, such as system edit checks. Specifically, managers monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts. Monitoring and evaluation activities can include unannounced examinations, site visits, covert testing, and surveys of stakeholders responsible for fraud controls. In addition, effective managers of fraud risks collect and analyze data, including data from reporting mechanisms and instances of detected fraud, for real-time monitoring of fraud trends and identification of potential control deficiencies (see section 4.3 below for further discussion on improving fraud risk management activities). The text box elaborates on monitoring and evaluation as types of assessments and on differences between the two.

Overview of Monitoring and Evaluation Activities

Evaluations, like monitoring activities, are reviews that focus on the program's progress towards achieving the objectives of fraud risk management. However, evaluations differ from monitoring activities in that they are individual systematic studies conducted periodically or on an ad hoc basis that are typically more in-depth examinations to assess the performance of activities and identify areas of improvement. As a result, designing evaluations involves considering whether a credible evaluation can be conducted in the time and with the resources available and, if not, what alternative information could be provided. For instance, in choosing between using existing data or conducting a survey, a manager might consider whether (1) the new information collected through a survey would justify the extra effort required, or (2) a high-quality survey can be conducted in the time available.[a]

Monitoring activities, because of their ongoing nature, can serve as an early warning system for managers to help identify and promptly resolve issues through corrective actions and ensure compliance with existing legislation, regulations, and standards. Moreover, monitoring enables a program to quickly respond to emerging risks to minimize the impact of fraud. According to the Australian National Audit Office, the timely monitoring and reporting of key issues and trends may have a higher priority than the precise accuracy of underlying data, particularly for high-risk initiatives. The results of monitoring and evaluations are useful insofar as the program uses them to improve fraud risk management activities.

[a]See GAO, *Designing Evaluations: 2012 Revision (Supersedes PEMD-10.1.4)*, GAO-12-208G (Washington, D.C.: Jan. 31, 2012).

Managers who effectively monitor and evaluate employ a risk-based approach to such activities by taking into account identified risks, emerging risks, as well as other internal and external factors that can influence the control environment.[58] For instance, changes within a program, including new initiatives, evolving technologies, and employee turnover, can affect the extent to which controls are effective or appropriate for addressing fraud risks. In addition, external factors, such as new fraud schemes, changes in legislative requirements, or economic instability may require managers to modify specific control activities. Moreover, some agencies or programs may not have direct control over certain control activities, and instead rely on external parties, such as other agencies or contractors, to design and implement fraud controls. In such circumstances, the extent of managers' influence over control activities may affect the level of risk, as managers may play more of an oversight role over fraud risk management activities. To help managers perform risk-based monitoring and evaluation in these situations, effective managers engage stakeholders who are responsible for fraud risk management activities in review processes.[59] For example, external entities can aid managers in field-testing or monitoring the effectiveness of control activities they implement or directly oversee, such as processes for validating self-reported data or reporting mechanisms.[60] In addition to reducing the risk of ineffective fraud controls, field-testing also helps to ensure that new controls do not improperly deny benefits, services, or contracts to legitimate recipients.

4.2 Monitor and Evaluate Fraud Risk Management Activities with a Focus on Measuring Outcomes

Effective monitoring and evaluation focuses on measuring outcomes and progress toward the achievement of objectives, rather than simply reviewing outputs and progress in implementing control activities. In general, managers who evaluate fraud risk management activities develop an understanding of the inputs, activities or processes, outputs, and outcomes for achieving antifraud objectives.[61] Federal law requires agencies to establish outcome-oriented goals and, as appropriate, a balanced set of performance indicators, including output and outcome indicators, to be used in measuring or assessing progress toward goals.[62] Moreover, accounting for short-term and intermediate outcomes can help managers to identify precursors that may be more readily measured than ultimate benefits (i.e., long-term outcomes), which may take years to achieve. For example, in addition to measuring the number of fraud-awareness trainings they conduct (an output), managers who evaluate short- or medium-term outcomes would also assess the results or change in behavior following the trainings, such as the number of hotline referrals related to a specific fraud scheme covered in the training. Managers may articulate the long-term outcome for managing fraud risks in different ways, but the outcome will likely reflect the objective of managing fraud risks, which generally aims to ensure program integrity and the effective provision of funds and services.

Managers may face challenges when monitoring and evaluating outcomes of fraud risk management activities. OMB highlights several reasons for this that are not unique to fraud risk management. For instance, according to OMB, managers are more likely to measure performance against outputs rather than outcomes, because outputs typically correspond to activities under managers' direct control and agencies are more likely to collect output data. In addition, managers might find it difficult to measure the performance of individual control activities because each control is one of many contributors to the long-term outcome, and therefore each control's effect may be difficult to isolate. Moreover, as noted, the deceptive nature of fraud can make it difficult to measure the extent of fraud in a reliable way, which can affect managers' capacity to evaluate outcomes and establish baselines, among other activities (see app. II for further discussion on challenges).

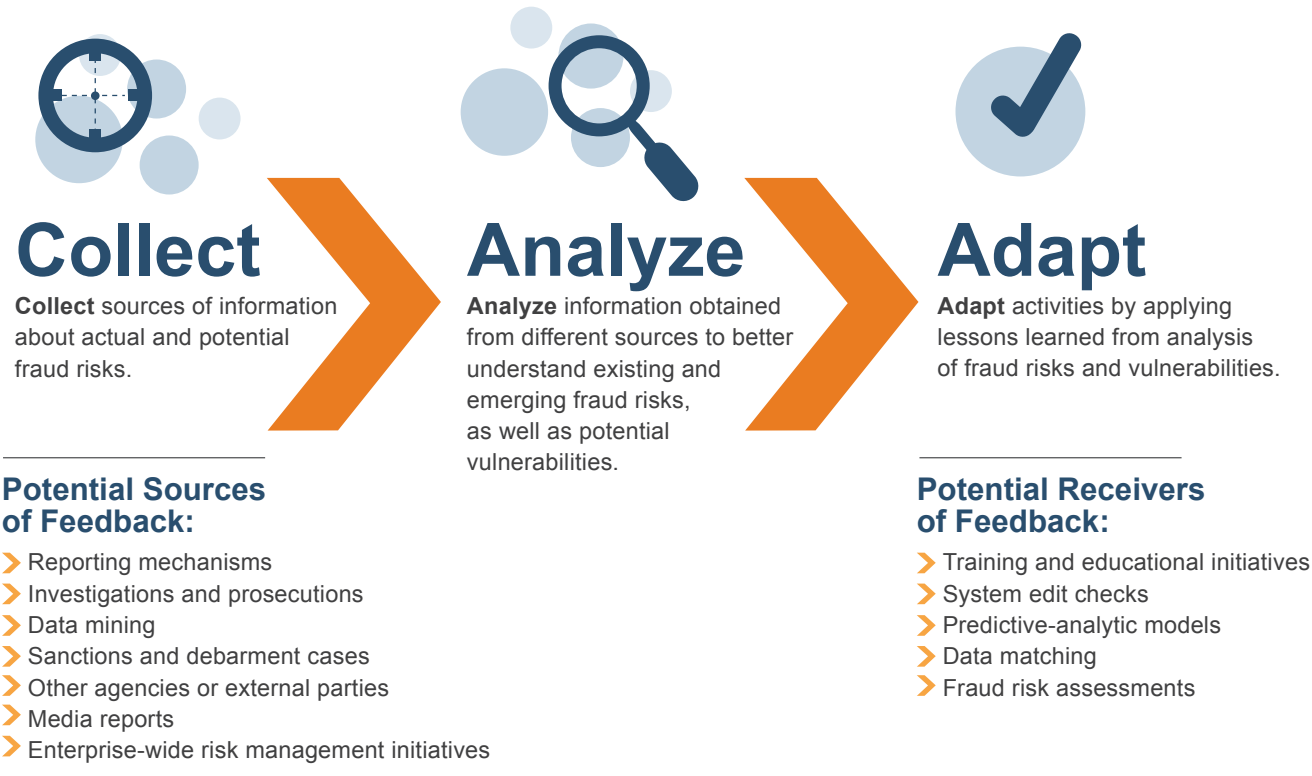
Managers' approach for addressing such challenges will vary based on factors like the employees' skills and expertise in measuring fraud losses, as well as the specific fraud risk management activity. In the absence of sufficient data to directly observe the effect of particular initiatives on mitigating fraud risks, managers can assess how well they followed recommended leading practices for designing fraud risk management activities, such as those described in the Framework.[63] For instance, managers can assess how well their efforts followed leading practices for designing a fraud risk assessment, antifraud strategy, and specific control activities. In addition, managers may consider using the fraud risk profile as a baseline in the absence of tangible measurements of the amount of fraud (for further discussion on the fraud risk profile, see the "Assess" section above).[64] The profile can serve as an internal benchmark to aid managers in assessing performance of fraud control activities with respect to changes in the perceived likelihood and impact of the fraud risks.

4.3 Adapt Fraud Risk Management Activities and Communicate the Results of Monitoring and Evaluations

Effective managers of fraud risks use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities. *Federal Internal Control Standards* requires managers to correct identified control deficiencies following monitoring and evaluations.[65] For instance, managers can improve the effectiveness of fraud-awareness trainings and other educational initiatives after surveying employees, if the survey responses indicate that comprehension of fraud-related issues is lower than intended. In addition, they can use information gained to improve the design of controls after conducting unannounced examinations or site visits of stakeholders responsible for fraud controls, including contractors. These practices illustrate the "Evaluate and Adapt" component of the Framework.

As noted above, as a leading practice, managers collect and analyze data on fraud trends and control deficiencies, a process that reflects the "lessons learned" element of monitoring and evaluation. After doing so, effective managers of fraud risks then use the analysis of identified instances of fraud and fraud trends to improve fraud risk management activities. In particular, managers use the analysis to prioritize and take corrective actions and enhance fraud-awareness trainings.[66] Similarly, effective managers of fraud risks use the results of investigations and prosecutions to adapt fraud risk management activities, including efforts to prevent and detect fraud. Generally, these processes are examples of feedback mechanisms, which allow managers to continually incorporate new information, such as changing risks or the effect of actions taken to mitigate risks and address vulnerabilities. According to entities we interviewed and literature we reviewed, various "sources" and "receivers" of feedback exist, as illustrated in figure 6.

Figure 6: Incorporating Feedback to Continually Adapt Fraud Risk Management Activities



Source: GAO. | GAO-15-593SP

Note: The examples of activities in this figure are for illustrative purposes only and are not meant to be an exhaustive list of opportunities to create feedback loops. In addition, some of the examples may fall under both the "source" and "receiver" categories. For example, a program manager may improve data-mining efforts based on feedback from reporting mechanisms and investigations. In addition, managers may receive information about fraud risks and trends during trainings, which can then be used to improve other preventive activities.

Effective managers of fraud risks communicate lessons learned from fraud risk management activities and corrective actions taken, if any, to relevant stakeholders. For instance, officials from the World Bank highlighted case studies, antifraud handbooks, and discussion groups as potential mechanisms for communicating feedback to enhance preventive activities. In addition, antifraud experts we interviewed noted trainings, newsletters, and the program's website as additional mechanisms for disseminating the results of reviews and investigations. Communicating the results of monitoring activities and evaluations can promote collaboration across the organization and with the OIG (see the "Design and Implement" section for further discussion on collaboration). Moreover, according to literature we reviewed, publicizing the results of evaluations of fraud control efforts can have a deterrent effect that can aid in fraud prevention.

Appendix I: Objective, Scope, and Methodology

This study describes leading practices for managing fraud risks that are applicable to federal government programs and can assist managers in making further progress towards effective fraud risk management.

To address this objective, we (1) collected information from interviews, focus groups, a literature review, and recommended reading; (2) analyzed the information and applied criteria we developed for leading practices; and (3) sought additional validation of our leading practices from government officials, as described in further detail below.

Information Collection

Interviews. We conducted interviews with 22 entities with experience across sectors, including officials with the Offices of Inspector General (OIG) of eight federal agencies, the Council of the Inspectors General for Integrity and Efficiency, three national audit offices of other countries, and 10 additional external entities, including the World Bank and the Organisation for Economic Co-operation and Development (OECD).[67]

- We selected OIGs of the five largest federal agencies by outlays, as well as the five largest grant-making agencies.[68] We identified the agencies using data from the Office of Management and Budget (OMB) for outlays from fiscal year 2013, the most recent year available at the time of our selection, and a GAO report issued in July 2014 about internal controls in agencies with the highest grant obligations.[69] The eight OIGs we interviewed include offices of the Department of Agriculture, the Department of Defense, the Department of Education, the Department of Health and Human Services, the Department of Housing and Urban Development, the Department of the Treasury, the Department of Transportation, and the Social Security Administration.
- We selected the national audit offices and external antifraud experts based on our review of relevant reports published by these entities, and recommendations from subject-matter experts within GAO. Specifically, we selected three national audit offices that published reports related to our objective. We selected external antifraud experts that represented different sectors, including private companies that have forensic services and accounting units with expertise in fraud risk management, state and local audit associations, nonprofit organizations, and intergovernmental organizations. The entities we selected also had expertise in areas related to fraud risk management, such as audits, investigations, trainings, the design and implementation of fraud controls, and developing integrity frameworks.

Focus groups. We attended a prominent antifraud conference and conducted three focus groups of 7 to 10 participants each that we screened for expertise relevant to fraud risk management. Two focus groups consisted of fraud risk management experts that presented at the conference, and one focus group involved conference participants with experience in preventing, detecting, and responding to fraud, or were otherwise studying or evaluating fraud and fraud control systems. Participants of the focus groups worked in different industries, including the private sector, academia, as well as federal, state, and local government. We moderated discussions of each focus group that aimed to elicit participants' views on the key elements of effective fraud risk management and challenges to employing effective fraud control.

Literature review and recommended reading. We conducted an extensive literature review, which included consideration of reports, journal articles, and books related to fraud risk management. We reviewed various sources, including (1) publications identified during a formal literature review, aided by a GAO research librarian; and (2) literature recommendations from external experts, entities we interviewed, and discussions with GAO experts. Our literature review included a search for keywords in several databases of peer-reviewed articles and books, and we limited our results to publications from January 1, 2011, to the summer of 2014, when we conducted the search.[70] As a result of this search, we ultimately identified 68 publications for in-depth review of practices related to fraud risk management.[71] In addition to the literature review, we also selected and reviewed 11 publications from a list of sources recommended by external and internal experts we interviewed. In all, we reviewed a total of 79 publications from our literature review and recommended literature. As part of our research, we considered existing frameworks and guides related to fraud risk management and integrity, including publications by the Australian National Audit Office, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the OECD, as well as the Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners (ACFE), among others.[72]

Analysis and Criteria for Leading Practices

We conducted a content analysis on the information we collected from the sources above by first compiling a list of practices for managing fraud risks from those sources.[73] We used NVivo, a qualitative-analysis software program, to facilitate this process of identifying and aggregating practices. We also categorized the practices according to two source types—testimonial and documentary—to facilitate analysis and application of the criteria described below. Our testimonial information came from a total of 25 sources, including 22 interviewees and three focus groups.[74] The documentary sources included the 79 publications identified during our literature review as well as recommended reading. We defined a practice as a leading practice for effectively managing fraud risks in the federal government if it was described as a leading practice, essential, or presented as highly important for managing fraud risks in at least one source of each source type—testimonial and documentary—or was presented in a similar fashion in at least three sources of one source type. In addition, we assessed whether the practices were relevant to fraud risk management in U.S. federal programs.

To determine whether a practice was relevant to U.S. federal programs, we applied professional judgment when analyzing practices, and we sought validation of leading practices from programs within federal agencies (see next section for additional details). In addition, we considered other factors when analyzing the importance of a particular practice or concept for effectively managing fraud risks, such as whether the statements were broadly applicable or limited to certain circumstances. We also took into account the possibility that our sources may not have addressed a specific practice related to fraud risk management that could in fact be considered leading or essential. We mitigated the risk of omitting leading practices by seeking validation from external entities, as described below. Moreover, we considered contradictory information when analyzing the practices, and used professional judgment to resolve any discrepancies.

Validation of Leading Practices and Technical Comments

To validate our list of leading practices, we sent a draft of the study to agency program officials associated with the same agencies as the OIGs we interviewed. In addition, we sent the draft Framework to the Small Business Administration in order to gain the perspective of an agency with the smallest amount of outlays in the OMB data we used for selecting agencies.[75] We requested that program officials review the draft Framework because federal program managers are the

primary intended users of the Framework, and we did not interview or include information from agency program officials as part of our initial data collection efforts. Therefore, program officials served as an independent source of validation. Specifically, we requested that each program office provide comments on: (1) whether the leading practices presented seemed relevant to their program and feasible to implement; (2) any additional information we should consider regarding specific practices or aspects of the Framework; and (3) information on additional practices not covered in the draft that would be beneficial or that their program employs. The following agencies and programs reviewed the draft Framework and provided comments as part of the validation process:[76]

- Department of Defense, Defense Contract Management Agency;
- Department of Education, Office of the Secretary, Risk Management Service, with input from the Office of Federal Student Aid and the Office of Special Education and Rehabilitative Services;
- Department of Health and Human Services, Assistant Secretary for Financial Resources;[77]
- Department of Housing and Urban Development, Office of Risk Management;
- Department of the Treasury, Internal Revenue Service, Return Integrity and Compliance Services;
- Small Business Administration, Office of Credit Risk Management; and
- Social Security Administration, Office of Anti-Fraud Programs.

In addition to the validation process described above, we also sent the draft Framework to selected entities for technical comments, including a fraud risk management task force sponsored by COSO and ACFE. These comments were not part of the formal validation process; however, this process helped to ensure the accuracy and completeness of the draft Framework.

We conducted our work from March 2014 to July 2015 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objective. The framework requires that we plan and perform our work to obtain sufficient and appropriate evidence to meet our stated objective and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any conclusions in this product.

Appendix II: Challenges Related to Measuring Fraud

The deceptive nature of fraud can make it difficult to measure outcomes of fraud risk management activities in a reliable way.

Specifically, as noted, managers may face challenges in measuring the extent of fraud in their programs, which can make it difficult to implement certain activities and determine their effectiveness in mitigating fraud risks. For instance, difficulties in estimating the extent of fraud can affect managers' abilities to conduct fraud risk assessments, establish baselines, evaluate outcomes, and fully consider the benefits and costs of control activities. This challenge is not unique to fraud. Managers face similar challenges in other settings that deal with risk and uncertainty, such as banking, intelligence, counterterrorism, natural disasters, and community health and safety. The following are examples of factors that can contribute to this challenge.

The extent of deterred fraud. The extent of fraud can be difficult to measure because of the likelihood that some activities serve a deterrent effect. For instance, in October 2012, we reported on the Centers for Medicare & Medicaid Services' (CMS) implementation of its Fraud Prevention System (FPS) and noted difficulties in measuring the amount of costs the agency avoided as a result of the system deterring would-be fraudsters.[78] Notwithstanding these difficulties, we identified ways for CMS to measure the outcomes of preventive activities and define quantifiable benefits from using FPS.

Isolating potential fraud from legitimate activity or other forms of improper payments. The full benefits of fraud risk management activities can be difficult to measure because of challenges in distinguishing potential fraud from legitimate activity or other forms of improper payments, such as waste and abuse. For example, in January 2015, we reported on the Internal Revenue Service's (IRS) efforts to combat fraudulent identity-theft refunds using data matching.[79] We highlighted the difficulties IRS officials have in determining, without conducting a tax-return audit, whether mismatches are attributable to identity theft or other types of noncompliant returns (i.e., a legitimate taxpayer makes a mistake or purposely files a noncompliant return). As a result, IRS officials based their estimate of the extent of fraud on certain assumptions they developed from analyzing past cases of identity-theft refund fraud.[80]

Undetected fraud. Challenges in determining the amount of undetected fraud can make it difficult to create accurate fraud estimates. For instance, in the aforementioned report, we said the IRS had been unable to estimate the amount of identity-theft refund fraud from undetected schemes, such as situations when there is no reported information to verify income. The IRS had considered different approaches to estimating the costs of undetected identity theft; however, we noted administrative costs and taxpayer burden are likely to make these approaches impractical.

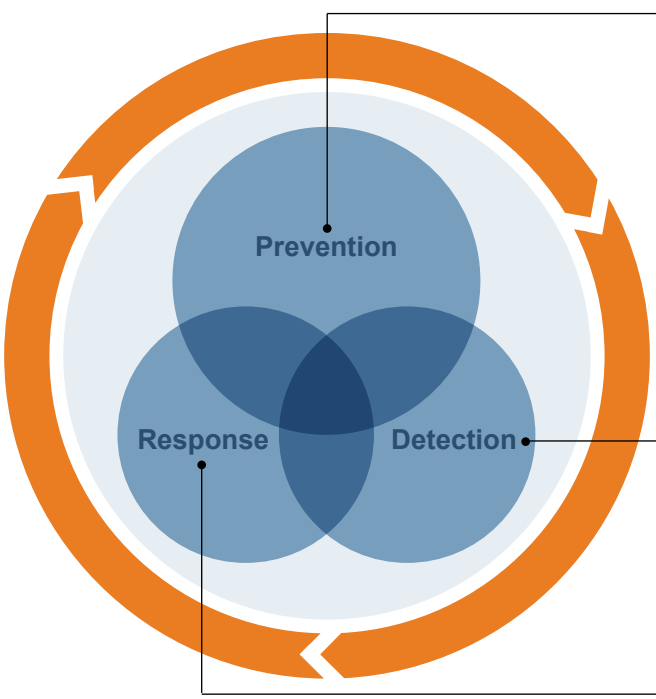
As discussed, managers' approach for addressing such challenges will vary based on factors like the employees' skills and expertise in measuring fraud losses and the specific fraud risk management activity. See the "Evaluate and Adapt" section above for further discussion on addressing this challenge.

Appendix III: Examples of Control Activities and Additional Information on Leading Practices for Data Analytics and Fraud-Awareness Initiatives

Examples of Control Activities

Control activities for managing fraud risks include the policies, procedures, techniques, and mechanisms related to three categories of control activities that are interdependent and mutually reinforcing—prevention, detection, and response. For instance, response activities, like investigations and prosecutions, also serve a preventive purpose by sending the message that managers will not tolerate fraud and creating the perception of punishment to deter fraudulent behavior. In addition, detection efforts can inform preventive activities, such as using data on instances of fraud identified through reporting mechanisms to enhance fraud-awareness training. Figure 7 shows examples of controls and activities within their primary categories. The examples are meant only to illustrate the range of control activities within each category and are not meant to be exhaustive. As noted, the specific control activities programs employ may differ based on a number of factors. These factors could include specific threats the program faces and risks it incurs; differences in objectives; managerial judgment; size and complexity of the entity; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance. Moreover, legislation, regulations, or other guidance may direct managers to implement certain control activities. As a result, managers may need other control activities than those shown in figure 7.

Figure 7: Examples of Controls and Activities to Prevent, Detect, and Respond to Fraud



Mitigate the risk of fraud occurring
- Antifraud strategy
- Employee background checks
- Fraud-awareness trainings
- System edit checks
- Data matching to verify eligibility
- Predictive analytics
- Segregation of duties
- Standards of conduct
- Transaction limits

Discover potential fraud that has already occurred[a]
- Audits
- Data matching after payments have been made
- Data mining
- Document reviews
- Hotlines and other reporting mechanisms
- Site visits

Investigate potential fraud, take corrective actions, and remedy the harm caused by fraud[a]
- Investigations
- Prosecutions
- Disciplinary actions
- Suspensions and debarments
- Payment recoveries

Source: GAO. | GAO-15-593SP

[a]In addition to program managers, other entities may also serve an important role in detecting and responding to fraud. For instance, an agency's Office of Inspector General (OIG), if applicable, is generally responsible for, among other things, conducting fraud-related audits and investigations. In addition, the Department of Justice or other law-enforcement entities may investigate instances of potential fraud. Moreover, federal attorneys and courts play an important role in fraud prosecutions.

Use Data-Analytic Tools and Techniques to Prevent and Detect Fraud

Data-analytics activities can include a variety of techniques to prevent and detect fraud. For example, data mining and data-matching techniques can enable programs to identify potential fraud or improper payments that have already been awarded, thus assisting programs in recovering these dollars, while predictive analytics can identify potential fraud before making payments.[81] As with other control activities, managers who effectively manage fraud risks take a risk-based approach to data analytics, considering the benefits and costs of investing in specific data-analytic tools and techniques and focusing data analytics on the program's highest risks.[82]

Federal Internal Control Standards states that managers should use quality information to achieve the entity's objectives. To do this, managers may identify information requirements, obtain relevant data from reliable internal and external sources, and process data into information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis.[83] The following leading practices can help enable managers to effectively use data to achieve the objective of mitigating the likelihood and impact of fraud.

Build support within the program. To be effective, data-analytics initiatives need support across the program and, in particular, from program managers. Beginning with small, short-turnaround projects that produce "small wins" can demonstrate the value of data-analytics initiatives.

Ensure employees have sufficient knowledge, skills, and training to perform data analytics. Managers who effectively implement data-analytics initiatives ensure that they have employees who understand how to use the data to perform data analytics. The agency's Office of Inspector General (OIG) may provide information for analyzing data for potential fraud, such as fraud indicators; however, as with the fraud risk assessment, the OIG should not implement data-analytics initiatives on behalf of a program in order to maintain its independence.

Combine data across programs and from separate databases within the agency to facilitate reporting and analytics, if legally permissible. Effective data-analytics initiatives combine data from various sources within the agency, which can enable managers to identify potential instances of fraud that may not be evident when analyzing data from separate programs or within separate databases. Centralizing data-analytics activities into one location can facilitate the use of data to identify potential instances of fraud and save resources.

Pursue access to necessary external data, including pursuing data-sharing agreements. Using data from other federal agencies or third-party sources can help managers identify potential instances of fraud. Specifically, data sharing allows entities that make payments—for example, to contractors, vendors, or participants in benefit programs—to compare information from different sources to help ensure that payments are appropriate. In 2013, we reported that participants of a data-analytics forum we held cited challenges agencies face in sharing data, including statutory requirements that place procedural hurdles on agencies wishing to perform data matching to detect fraud, as well as technical obstacles that make it more difficult to share available data, such as the lack of uniform data standards across agencies.[84]

Consider program rules and known or previously encountered fraud schemes to design data-analytic tests. The specific data-analytic tests that will be most effective in helping managers prevent or detect potential fraud will vary by program because of the different fraud risks programs face. By using information on previously encountered fraud schemes or known fraud risks, managers can identify signs of fraud (i.e., red flags) that may exist within their data. For example, if program rules prohibit individuals from making purchases over a certain dollar amount, testing transaction data to identify multiple purchases from the same cardholder to the same vendor in the same day could identify cardholders splitting purchases to circumvent the purchase limit. In addition, as discussed in the "Evaluate and Adapt" section, effective fraud risk managers collect and analyze data on identified fraud schemes and use these lessons learned to improve fraud risk management activities. For instance, managers may revise data-analytic tests based on newly encountered fraud schemes to better identify these schemes in the future.

Data-analytics knowledge and experience can vary across programs, and, as with other control activities, collaboration with stakeholders can help ensure the effectiveness of data-analytics activities. For instance, involving legal experts can help managers understand legal requirements to protect privacy or help managers pursue access to external data, and collaborating with the OIG can help improve the design of data-analytic tests, as OIGs can share information on fraud risks and indicators. Further, in comments on a draft of this study, officials from one agency stated that seeking support from the agency's chief information officer can help program

managers develop data-analytic tools and help program managers avoid duplicative software purchases.

As noted, data-analytics activities can include a variety of techniques. Managers who effectively manage fraud risks design and implement the following data-analytic techniques that are broadly applicable to agencies.

Apply system edit checks to help ensure data meet requirements before data are accepted into the program's system and before payments are made. System edit checks are instructions programmed into an information-processing system to help assure that data are complete, accurate, valid, and recorded in the proper format, such as checks to identify missing data, incorrect data, or erroneous dates. System edit checks can be used to compare data entries to requirements, and automatically deny entries that do not meet requirements or flag them for further review. For example, we previously found that Medicare aims to reduce inappropriate payments by using edit checks that deny payment for services where the quantity billed is at a level not likely to be provided under normal medical practice, such as daily doses of drugs higher than the maximum amounts in the prescribing information or services that are anatomically impossible, like performing more than one appendectomy on the same beneficiary.[85] In addition, we have found that the Internal Revenue Service (IRS) uses edits to automatically reject tax returns filed using a given Social Security number (SSN) after IRS receives an electronically filed return for that SSN.[86]

Conduct data matching to verify key information, including self-reported data and information necessary to determine eligibility. To effectively prevent and detect instances of potential fraud, managers take steps to verify reported information, particularly self-reported data and other key data necessary to determine eligibility for enrolling in programs or receiving benefits.[87] Specifically, managers conduct data matching using government or third-party sources to verify data electronically. For example, if a firm reports that it is a small business in order to receive federal contracts, an agency can use third-party data sources to verify that the firm actually meets requirements to qualify as a small business. In addition to verifying initial eligibility, data matching can enable programs that provide ongoing benefits to identify changes in key information that could affect continued eligibility.

Conduct data mining to identify suspicious activity or transactions, including anomalies, outliers and other red flags in the data. Activity or transactions that deviate from expected patterns can potentially indicate fraudulent activity. Therefore, managers who effectively use data analytics to detect potential fraud look for unusual transactions or data entries that do not fit an expected pattern. Specifically, applying filters or predefined rules to transactions can help identify those that exhibit signs of fraud.

To help ensure these techniques are implemented effectively, effective managers automate data-analytic tests to monitor data for fraud indicators on a continuous, real-time basis. Automating aspects of data-analytics initiatives, such as system edit checks and applying fraud filters to identify red flags, can provide information on potential fraud in real time. In addition, because automated checks are less labor-intensive than traditional control mechanisms, such as manual checks, automating data-analytic tests can allow managers to monitor large amounts of data more efficiently.

In addition to these techniques, the text box describes an example of how one program uses another data-analytic technique—predictive analytics—to help prevent fraud.

Using Predictive Analytics to Help Prevent Fraud

In addition to the techniques described in this Framework, predictive-analytics techniques can help increase the effectiveness of antifraud programs. Predictive-analytics technologies include a variety of automated systems and tools that can be used to identify particular types of behavior, including potential fraud, before transactions are completed. As a result, these techniques can enable agencies to identify fraud before they make payments, rather than detecting fraudulent transactions and attempting to recover funds after payment.

We reported in 2012 that the Centers for Medicare & Medicaid Services (CMS) had implemented a system that uses historic Medicare claims and other data to identify high-risk claims in the Medicare fee-for-service program. The system includes predictive models, which aim to help identify providers with billing patterns associated with known forms of fraud. Specifically, the models use historical data to identify patterns associated with fraud, and then apply this information to current claims data. Predictive models require analysis of large amounts of data; however, these models can help enable CMS to detect patterns of behavior that individually may not be suspicious but, when conducted together, can indicate fraudulent activity.[a]

[a]GAO, *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012).

In addition to the practices above, managers also take the following steps to help ensure the results of data analytics can be used effectively:

Tailor the output of data analytics to the intended audience to help ensure the results are usable. This can help increase the likelihood that data-analytics initiatives will be effective. For example, experts from one organization we interviewed stated that presenting the results of data analytics in a graphic or visual manner can help individuals across the organization quickly understand how data analytics work and understand the value of data analytics. Similarly, several participants of the data-analytics forum we held in 2013 emphasized the importance of data visualization in showing the value of data analytics.[88] One participant stated that she worked with investigators to understand the information they need to conduct investigations and provided tailored information, rather than providing raw data and risk scores.

Review the results of data analytics and refer appropriate cases to the OIG for further investigation. This includes reviewing identified cases to remove false positives, such as by taking steps to verify the facts and circumstances of identified cases and checking for math or other errors.

While the leading practices described in this appendix can help managers design and implement effective data-analytic tools and techniques to prevent and detect potential fraud, these techniques alone may not be sufficient to ensure that ineligible individuals or entities do not fraudulently enroll in a program or receive benefits. Therefore, managers may need to combine data-analytics activities with additional controls. For example, physical inspections, site visits, or making contact with program enrollees or beneficiaries for additional information can also be used to help prevent and detect potential fraud.

Conduct Fraud-Awareness Initiatives to Prevent and Deter Fraud

Fraud-awareness initiatives include fraud training and education for managers, employees, and stakeholders with responsibility for implementing aspects of the program. Increasing fraud awareness among managers, employees, and stakeholders serves a preventive purpose by helping to create a culture of integrity and compliance within the agency. Further, increasing fraud awareness can enable managers and employees to better detect potential fraud.

To help ensure the effectiveness of fraud education and training programs, managers follow these leading practices:

Attend training. In addition to ensuring that managers have a sufficient awareness of fraud and are able to identify potential fraud, attending and participating in trainings allows managers to show their commitment to antifraud efforts.

Require all employees to attend training upon hiring and on an ongoing basis thereafter, and maintain records to track compliance. In addition, managers may consider tailoring training to the employee's role and level and providing more-frequent or more-targeted training to employees in high-risk positions or areas.

Collaborate with the OIG when planning or conducting training and promote the results of successful OIG investigations internally. OIGs have expertise in fraud issues within the agency. Collaborating with the OIG when planning or conducting training provides an opportunity for the OIG to share this expertise, such as information on fraud indicators and tools to combat fraud, and to aid in building fraud awareness within the agency.

Provide training to stakeholders with responsibility for implementing aspects of the program.[89] In addition to training for program employees, providing training to contractors, state employees, and others with responsibility for implementing aspects of the program can help increase fraud awareness among these entities and enhance prevention efforts. For example, we reported in December 2011 that CMS sponsors a training institute that provides free training, technical assistance, and support to states, as well as opportunities to develop relationships with program integrity employees from other states.[90]

Use multiple methods to educate employees and reinforce key antifraud messages. There are a variety of methods, in addition to formal training, that can be used to increase fraud awareness. Examples of educational activities related to fraud control include newsletters highlighting the results of cases or information on fraud schemes, fraud-indicator cards that communicate red flags to employees, or computer-based trainings that are available on-demand to employees, such as videos about fraud issues.

Convey fraud-specific information that is tailored to the program and its fraud risk profile. Managers may incorporate fraud training and education into existing ethics and compliance training; however, an effective training program includes fraud-specific information and is tailored to the program's fraud risk profile. Specifically, table 7 shows information conveyed through effective fraud trainings.

Table 7: Leading Practices for Developing and Conveying Training Content

	The definition of fraud and examples of specific types of fraud that employees are likely to encounter, illustrated by actual fraud cases.
	Information on how to identify fraud schemes, including use of red flags and risk indicators.
	Relevant legislation and policies.
	Expectations regarding ethical behavior, including information on the program's standards of conduct.
	Responsibilities for contributing to fraud risk management, including implementing fraud controls and reporting potential fraud.
	Information on how and where to report fraud, including information on reporting mechanisms, and what to report.
	A positive message, such as emphasizing the benefits of fraud risk management for the program.
	The cost of fraud to the program.
	Consequences of engaging in fraud, such as sanctions, disciplinary actions, and other punishments.

Source: GAO. | GAO-15-593SP

In addition to fraud training for employees and internal educational initiatives, effective fraud-awareness initiatives include efforts to increase awareness about program integrity and antifraud efforts outside the program, such as among program beneficiaries and the general public. Specifically, the following leading practice helps program managers to increase fraud awareness outside the program:

Publicize information on antifraud efforts and successfully resolved fraud cases. The expectation that government will detect and punish fraud helps deter would-be fraudsters. Publicizing information on antifraud efforts and successfully resolved cases helps deter individuals who may engage in fraudulent behavior by increasing awareness about likely detection and penalties for committing fraud. However, one source we reviewed noted, while an organization can help deter fraud by communicating that it has a comprehensive plan to detect fraud, the organization may want to keep specific detection procedures and techniques confidential so that potential perpetrators of fraud do not become aware of their existence.

In addition to serving a deterrent effect, increasing awareness about fraud schemes outside the program can help prevent fraud. For example, we previously found the IRS provides taxpayers targeted information, including tips and suggestions for safeguarding personal information, to help prevent tax-refund and employment fraud committed through identity theft.[91]

Appendix IV: Risk Factors for Assessing Improper-Payment Risk

The Improper Payments Information Act of 2002 (IPIA), as amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA), the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), and related guidance by the Office of Management and Budget, requires federal executive-branch agencies to, among other things, identify programs and activities that may be susceptible to significant improper payments—a process known as a risk assessment.[92] Agencies must institute a systematic method of reviewing and assessing their programs, which may take the form of either a quantitative analysis based on a statistical sample or a qualitative evaluation. The legislation and guidance require that agencies, in performing their risk assessments, take into account those risk factors that are likely to contribute to significant improper payments, including

1. whether the program or activity reviewed is new to the agency;

2. the complexity of the program or activity reviewed, particularly with respect to determining correct payment amounts;

3. the volume of payments made annually;

4. whether payments or payment-eligibility decisions are made outside of the agency, for example, by a state or local government, or a regional federal office;

5. recent major changes in program funding, authorities, practices, or procedures;

6. the level, experience, and quality of training for personnel responsible for making program-eligibility determinations or certifying that payments are accurate;

7. significant deficiencies in the audit reports of the agency, including but not limited to the agency Inspector General or the GAO report audit findings or other relevant management findings that might hinder accurate payment certification;

8. results from prior improper-payment work; and

9. inherent risk of improper payments due to the nature of the agency's programs or operations.[93]

Appendix V: Example of a Fraud Risk Profile

As noted, the fraud risk profile is an essential piece of the antifraud strategy, as described in the "Design and Implement" section, and informs the specific control activities managers design and implement. The elements in table 8 reflect key elements of fraud risk assessments and the fraud risk profile. The table is meant solely for illustrative purposes to show one possible format for agencies to document their fraud risk profile. The table shows information related to one fraud risk; however, a robust fraud risk profile would include information about all fraud risks that may affect a program. Documenting fraud risks together can aid managers in understanding links between specific risks. In addition, other tools a program uses to assess risks, such as the risk matrix discussed in the "Assess" section, can supplement the documentation for the fraud risk profile. We adapted the table and additional information below it from *Standards for Internal Control in the Federal Government*, as well as one publication by the Australian National Audit Office and one cosponsored by the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners.

Table 8: Elements of a Fraud Risk Profile for One Hypothetical Fraud Risk

	Insufficient automatic checks of databases and overreliance on manual checks that could introduce human error. Volume of applications causes excessive pressure to expedite approvals and results in less attention paid to verifying identities. Management override of control activities. Poor fraud awareness among supervisors and application reviewers.
	Examples include a five-point scale showing a range for likelihood, such as "rare" to "almost certain," as well as a range for impact, such as "immaterial" to "extreme."
	Examples include a five-point scale, such as "very low, low, medium, high, and very high," based on the product of the likelihood and impact of the inherent risk.
	Manual checks against databases with some automatic checks. Quarterly newsletters with fraud indicators related to identity theft. Supervisor approval required for suspicious applications.
	Examples include a five-point scale showing a range for likelihood, such as "rare" to "almost certain," as well as a range for impact, such as "immaterial" to "extreme."
	Examples include a five-point scale, such as "very low, low, medium, high, and very high," based on the product of the likelihood and impact of the residual risk.

Source: GAO, Australian National Audit Office, Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners. | GAO-15-593SP

Note: Information in this table is from *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014) (this version will be effective beginning with fiscal year 2016) and is also adapted from the Australian National Audit Office, *Fraud Control in Australian Government Entities: Better Practice Guide* (March 2011), and Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide* (n.d.).

[a]Information in this row relates to the antifraud strategy and the specific actions managers decide to take to avoid, share, accept, or reduce fraud risks based on their risk tolerance. See the "Design and Implement" section for additional information about using the fraud risk profile to inform the antifraud strategy.

The following is additional information about the elements in table 8.

Identified Fraud Risks. What fraud risks does the program face? Include a brief description of the fraud risk or scheme. This list will vary by program, and may be informed by activities to gather information during the fraud risk assessment, such as interviews with staff, brainstorming sessions, and information from hotline referrals.

Fraud Risk Factors. What conditions or actions are most likely to cause or increase the chances of a fraud risk occurring? This may reflect fraud risk factors highlighted in *Federal Internal Control Standards*, as well as other factors that provide additional details about specific fraud risks.

Fraud Risk Owner. Which group or individual within the program is responsible for addressing the risk? The owner of the fraud risk will vary by program, but generally, this is the entity with accountability for addressing the fraud risk.

Inherent Risk Likelihood and Impact. In the absence of controls, how likely is the fraud risk and what would the impact be if it were to occur? As noted in the "Assess" section, the specific methodology for assessing the likelihood and impact of risks will vary by agency. One option for assessing likelihood is to use a five-point scale, as noted in table 8. When considering impact, participants of the fraud risk assessment may consider the impact of fraud on the program's compliance with laws and regulations, operations, and reputation.

Inherent Risk Significance. In the absence of controls, how significant is the fraud risk based on an analysis of the likelihood and impact of the risk? While the specific methodology for assessing risks may vary by agency, including qualitative and quantitative methodologies, managers may multiply the likelihood and impact scores, or apply a five-point scale.

Existing Antifraud Controls. What controls does the program already have in place to reduce the likelihood and impact of the inherent fraud risk? This is intended to assist with mapping the existing controls to the fraud risks or schemes that would reduce the likelihood and impact of a fraud risk occurring.

Residual Risk Likelihood and Impact. Taking into account the effectiveness of existing controls, how likely is the fraud risk and what would the impact be if it were to occur? Managers may consider assessing both the residual likelihood and impact of fraud risks using the five-point scale described in table 8. Controls that are not properly designed or operating effectively may contribute to high residual risk.

Residual Risk Significance. How significant is the fraud risk based on an analysis of the likelihood and impact, as well as the effectiveness of existing controls? Like inherent risk significance, qualitative and quantitative methodologies may be used to establish residual risk significance.

Fraud Risk Response. What actions does the program plan to address the fraud risk, if any, in order to bring fraud risks within managers' risk tolerance? Information in this row relates to the antifraud strategy and the specific actions managers decide to take to avoid, share, accept, or reduce fraud risks.

Appendix VI: Endnotes

Introduction

[1]Fraud involves obtaining something of value through willful misrepresentation (see GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G [Washington, D.C.: Sept. 10, 2014], 8.02, for discussion on types of fraud). Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk. For the purposes of this study, unless noted otherwise, we generally use the term "fraud" to include potential fraud for which a determination has not been made through the judicial or other adjudicative system.

[2]An improper payment is defined as any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. It includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts. Office of Management and Budget (OMB) guidance also instructs agencies to report as improper payments any payments for which insufficient or no documentation was found. It is important to note that reported improper payment estimates may or may not represent a loss to the government. The Improper Payments Information Act of 2002 (IPIA), as amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA) and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), requires federal executive-branch agencies to, among other activities, identify programs and activities that may be susceptible to significant improper payments, estimate the annual amount of improper payments for those programs and activities, and take actions to reduce improper payments. Hereafter we refer to these acts as "improper-payment legislation."

[3]GAO, *State Department: Pervasive Passport Fraud Not Identified, but Cases of Potentially Fraudulent and High-Risk Issuances Are under Review*, GAO-14-222 (Washington, D.C.: May 1, 2014) and *State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud*, GAO-10-922T (Washington, D.C.: July 29, 2010).

[4]OMB issued its most-recent guidance in October 2014 called Memorandum No. M-15-02, app. C to Circular No. A-123, *Requirements for Effective Estimation and Remediation of Improper Payments* (Oct. 20, 2014). At the time of issuance of the Framework, OMB was working on an update to this memorandum, which is expected to be issued later this year, according to an OMB official.

[5]According to OMB, enterprise risk management (ERM) is an "effective agency-wide approach to address the full spectrum of the organization's risks by understanding the combined effect of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that, when brought together, provides better insight about how to most effectively prioritize and manage risks to mission delivery." Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11, § 270 (2014).

[6]In fiscal year 2014, federal agencies reported an estimated $124.7 billion in improper payments, which includes payments made as a result of fraud, waste, and abuse. The estimate was attributable to 124 programs across 22 agencies. We have previously reported on opportunities for agencies to improve calculations of reliable improper-payment estimates, design and implement controls to prevent improper payments, and analyze their root causes.

[7]GAO, *SSA Disability Benefits: Enhanced Policies and Management Focus Needed to Address Potential Physician-Assisted Fraud*, GAO-15-19 (Washington, D.C.: Nov. 10, 2014). We recommended that the Social Security Administration (SSA) develop an implementation plan for new initiatives that use analytics and that includes, among other things, time frames for implementation, resources and staffing needs, and data requirements. SSA agreed with our recommendation and noted plans to develop a comprehensive plan that considers resourcing and staffing needs, available technology, and the integration of SSA's activities.

[8]GAO, *Improper Payments: DOE's Risk Assessments Should Be Strengthened*, GAO-15-36 (Washington, D.C.: Dec. 23, 2014). We recommended that the Department of Energy (DOE) take steps to improve its risk assessments, including revising guidance on how to address risk factors and providing examples of other risk factors likely to contribute to improper payments; DOE concurred with our recommendations.

[9]For instance, we reported on positive steps the Centers for Medicare & Medicaid Services (CMS) has taken to improve program integrity, such as demonstrating leadership commitment, and creating action plans that define root causes and steps to reduce improper payments in Medicare. However, as of our most recent High-Risk Series update issued in February 2015, all parts of the Medicare program are on OMB's list of high-error programs, suggesting additional actions are needed. For additional details, see GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[10]See Principle 8, "Assess Fraud Risks." *Standards for Internal Control in the Federal Government* are hereafter referred to as *Federal Internal Control Standards*. See GAO-14-704G. This version of *Federal Internal Control Standards* will be effective beginning with fiscal year 2016 (Oct. 1, 2015). The Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated its internal control guidance in 2013 with the issuance of a revised *Internal Control—Integrated Framework. Federal Internal Control Standards* adapts principles in the COSO guidance for the government environment.

[11]Improper-payment legislation and OMB guidance largely address financial fraud, such as beneficiary payments, and do not address nonfinancial fraud that federal programs may face, such as attempts to steal or misrepresent an identity to obtain a passport or avoid detection by authorities. In addition, legislation and guidance on improper payments require agencies to estimate the amount of potential improper payments that have already been made and develop corrective actions to address the causes of such payments in the future. As such, the legislation and guidance do not require agencies to assess and take steps to address fraud vulnerabilities if they have not identified potentially improper payments that have already occurred as a result of those vulnerabilities. Moreover, *Federal Internal Control Standards* includes principles and attributes that may be relevant for effective fraud risk management, but are not necessarily fraud-specific.

[12]A national audit office is the supreme audit institution of a country. Supreme audit institutions are national agencies responsible for auditing government revenue and spending. In general, the primary responsibility of a country's supreme audit institution is to oversee the management of public funds and the quality and credibility of the government's reported financial data. GAO is the national audit office of the United States.

[13]Two of the agencies, the Department of Agriculture and the Department of Health and Human Services, were included on both lists. Therefore, we interviewed the OIGs of a total of 8, rather than 10, federal agencies.

[14]For instance, see Australian National Audit Office, *Fraud Control in Australian Government Entities: Better Practice Guide* (March 2011); Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework* (New York: American Institute of Certified Public Accountants, 2013); Organisation for Economic Co-operation and Development, *Towards a Sound Integrity Framework: Instruments, Processes, Structures and Conditions for Implementation*, GOV/PGC/GF(2009)1 (Apr. 23, 2009); and Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide* (n.d.).

Framework Overview

[15]Risk management, broadly defined, is a process that helps agency managers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty to mitigate risks.

[16]Fraud risks can be managed and assessed at the program or agency level, given variation among programs within agencies. For the sake of consistency, we generally refer to programs throughout this study; however, the practices we discuss can apply to agencies as well. Managers decide whether to carry out each aspect of fraud risk management at the program level or agency level.

[17]"Pay-and-chase" refers to the practice of detecting fraudulent transactions and attempting to recover funds after payments have been made.

[18]As noted in *Federal Internal Control Standards*, control activities are the policies, procedures, techniques, and mechanisms that enforce managers' directives to achieve the entity's objectives and address related risks.

[19]Because investigating instances of potential fraud is generally the responsibility of OIGs or law-enforcement entities, rather than program managers, we do not describe leading practices for investigating potential fraud here. For additional information on standards and principles for conducting investigations, see Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Investigations* (Washington, D.C.: Nov. 15, 2011).

[20]Agencies may be subject to additional laws, regulations, or internal policies that affect their fraud risk management activities. For instance, the Small Business Jobs Act of 2010 requires the Centers for Medicare & Medicaid Services (CMS) to use specific data-

analytic techniques to identify and to prevent improper payments under the Medicare fee-for-service program. In addition, the National Defense Authorization Act for Fiscal Year 2012 required the Small Business Administration to make certain changes to its program policy directives for the Small Business Innovation Research Program and Small Business Technology Transfer program to prevent fraud, waste, and abuse.

[21]Computer Matching and Privacy Protection Act of 1988. Pub. L. No. 100-503. (Oct. 18, 1988). For our report on the forum, see: GAO, *Highlights of a Forum: Data Analytics for Oversight and Law Enforcement*, GAO-13-680SP (Washington, D.C.: July 15, 2013). Data matching is a process in which information from one source is compared with information from another, such as government or third-party databases, to identify any inconsistencies. See app. III for more information and leading practices on using data matching and other data-analytic techniques to prevent and detect fraud.

Commit

[22]Similarly, according to *Federal Internal Control Standards*, managers should demonstrate a commitment to integrity and ethical values and managers set the tone at the top (see GAO-14-704G, 1.01).

[23]GAO-14-704G, 3.02–3.05.

[24]Agency managers are not required to have a Chief Risk Officer or enterprise risk management function; however, according to OMB guidance, they are expected to manage risks to mission, goals, and objectives of the agency (see OMB, Circular No. A-11, § 270.25).

[25]See GAO-14-704G, 5.01.

[26]As noted in the "Assess" section, the OIG can inform fraud risk management activities and help managers identify fraud risks.

[27]See OMB, Circular No. A-11, § 270.25, for a list of roles and responsibilities of effective enterprise risk managers, which generally reflect the leading practices related to the roles and responsibilities of an antifraud entity.

[28]GAO, *Improper Payments: Reported Medicare Estimates and Key Remediation Strategies*, GAO-11-842T (Washington, D.C.: July 28, 2011).

Assess

[29]GAO-14-704G, 8.01–8.07.

[30]In accordance with improper payment legislation, agencies were required to conduct risk assessments for all federal programs and activities in fiscal year 2011 and at least once every 3 years thereafter for programs and activities deemed not risk susceptible. Moreover, OMB's implementing guidance requires agencies to reassess a program's risk during the next annual cycle, even if it is less than 3 years from the last risk assessment, if a program experiences a significant change in legislation or a significant increase in funding.

[31]See GAO-14-704G, OV2.15.

[32]As discussed, one leading practice is for the antifraud entity to spearhead the fraud risk assessment process. However, we refer to managers when describing the fraud risk assessment process in this section, because they are ultimately responsible for the overall fraud risk management in an agency.

[33]As noted, the process for assessing fraud risks may vary, depending on the circumstances within an agency or program. The five actions listed are critical for the risk assessment process; however, managers may not necessarily carry them out in the order described.

[34]According to *Federal Internal Control Standards*, inherent risk is the risk to an entity prior to considering management's response to the risk (see GAO-14-704G, 7.03).

[35]In addition to fraud, management should consider other forms of misconduct that can occur, such as waste and abuse (see GAO-14-704G, 8.03).

[36]GAO-14-704G, 8.04–8.05. In addition, improper-payment legislation and OMB guidance require agencies to take into account nine risk factors that are likely to contribute to significant improper payments (see app. IV for additional information).

[37]Terminology in the sources we reviewed for this activity varied. For instance, sources that discussed more rigorous quantitative analysis of fraud risks referred to "likelihood" as "probability" or "frequency" and "impact" as "consequence" or "percentage loss rate." For purposes of this study, we use "likelihood" and "impact," and we do not examine the differences between these terms and others' terms.

[38]OMB, Memorandum No. M-15-02, *Appendix C to Circular No. A-123, Requirements for Effective Estimation and Remediation of Improper Payments*, requires agencies to establish a systematic method for determining whether their risk of improper payments is significant, unless they receive approval from OMB to deviate from the step. The guidance notes that this method may be a quantitative evaluation based on a statistical sample or a qualitative method, such as a risk-assessment questionnaire.

[39]Estimates that describe the extent of fraud can be useful for assessing fraud risks; however, a precise number that represents fraud losses or benefits of preventive activities may not always be needed or appropriate for making an informed decision. As we note in our discussion of risk and uncertainty in GAO's *Cost Estimating and Assessment Guide*, for management to make good decisions about resource allocation, a cost estimate must reflect the degree of uncertainty, so that a level of confidence can be given about the estimate. For instance, in our report on identity-theft tax-refund fraud issued in January 2015, we stated that reporting a point estimate for revenue lost without a range or some other indication of uncertainty could provide a false sense of precision about refunds prevented and paid. We noted this false sense of precision could affect decisions about how to allocate resources to combat identity- theft refund fraud. GAO, *Identity and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks*, GAO-15-119 (Washington, D.C.: Jan. 20, 2015).

[40]Compliance risk is the potential for loss or other detrimental effects arising from violations of laws or regulations, or nonconformance with internal policies or ethical standards. Reputational risk is the potential for loss or other detrimental effects arising from negative publicity regarding an agency's practices.

[41]GAO-14-704G, 6.08.

[42]In addition to risk tolerance, risk appetite is another concept in risk management that describes the amount and type of risk that an organization is willing to accept in pursuit of its objectives. In this study, we focus on one type of risk, and managers of federal programs will generally have a low risk appetite for fraud, regardless of the circumstances. For these reasons, we do not explore the concept of risk appetite in our discussion of risk tolerance. See Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management—Understanding and Communicating Risk Appetite* (January 2012) for further discussion on risk appetite and risk tolerance.

[43]GAO-14-704G, 6.09.

[44]In addition to the effectiveness of the program's own control activities, in some instances the residual risk may depend on the effectiveness of controls implemented by other agencies or programs, such as in programs that allow individuals to enroll based on the individual receiving benefits from another federal program.

Design and Implement

[45]OMB guidance states that managers must carefully assess the appropriate balance between controls and risk in their programs and operations and must ensure an appropriate balance between the strength of controls and the relative risk associated with particular programs and operations. Office of Management and Budget, *Management's Responsibility for Internal Control*, Circular No. A-123 (revised Dec. 21, 2004).

[46]See GAO-14-704G, 7.08. "Accept" means no action is taken to respond to the risk based on the insignificance of the risk. "Reduce" refers to an action that is taken to reduce the likelihood or magnitude of the risk. "Share" suggests an action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses. Finally, "Avoid" indicates an action is taken to stop some or all of the operational process causing the risk. In particular, *Federal Internal Control Standards* notes that it may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes, such as by reallocating roles among personnel to enhance segregation of duties.

[47]GAO-14-704G, 3.09–3.12. Moreover, *Federal Internal Control Standards* requires managers to design specific actions for responding to identified risks (see GAO-14-704G, 10.01).

[48]GAO-14-704G, OV4.07.

[49]For guidance on using these techniques, see Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Circular No. A-94, Revised (Washington, D.C.: Oct. 29, 1992). For additional guidance on determining costs, see GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP, (Washington, D.C.: March 2009).

[50]*Federal Internal Control Standards* says managers should consider designing appropriate types of control activities for the entity's internal control system. Factors that may affect the specific control activities used by an entity include: specific threats the entity faces and risks it incurs; differences in objectives; managerial judgment; size and complexity of the entity; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance. GAO-14-704G, 10.03.

[51]GAO-14-704G, 10.01.

[52]For instance, programs that provide assistance in the form of cash or a cash equivalent, such as a credit or debit card, may manage fraud risks, in part, by obtaining signatures from cash recipients. We determined that such examples of control activities, while useful for combating fraud, are context-specific and thus not discussed in detail in this study. App. III provides an overview of additional control activities related to fraud prevention, detection, and response.

[53]GAO-14-704G, 10.12–10.14.

[54]As previously noted, we generally use the term "fraud" in this study to include potential fraud for which a determination has not been made through the judicial or other adjudicative system, unless noted otherwise.

[55]Suspensions and debarments are tools that agencies may use to protect the government's interests by excluding individuals, contractors, and grantees from receiving federal contracts, grants, and other forms of financial assistance based on various types of misconduct. The Federal Acquisition Regulation (FAR) establishes the policies and procedures governing suspension and debarment actions related to federal contracts. The Nonprocurement Common Rule establishes the policies and procedures governing suspension and debarment for discretionary nonprocurement awards (i.e., grants, cooperative agreements, scholarships, or other assistance). The FAR and the Nonprocurement Common Rule specify numerous causes for suspensions and debarments, including fraud, false statements, theft, bribery, tax evasion, and any other offenses indicating a lack of business integrity (see FAR §§ 9.406-2 and 9.407-2 and 2 C.F.R. §§ 180.700 and 180.800). In addition, OMB has the authority to issue guidelines for nonprocurement suspensions and debarments, and the Office of Federal Procurement Policy within OMB provides overall direction for government-wide procurement policies, including those on suspensions and debarments under the FAR. See GAO, *Suspension and Debarment: Some Agency Programs Need Greater Attention, and Governmentwide Oversight Could be Improved*, GAO-11-739 (Washington, D.C.: Aug. 31, 2011) for our review of characteristics of active suspension and debarment programs.

[56]See GAO-14-704G, 14.01–15.09, for related principles and attributes.

[57]We recommended that the agency identify ways to remove potential disincentives for detecting and referring potential fraud. The agency partially agreed with the recommendation and stated that it would continue to encourage its employees to report potential fraud and give them the tools needed to be successful. See GAO-15-19.

Evaluate and Adapt

[58]As noted in *Federal Internal Control Standards*, the scope and frequency of evaluations depend primarily on the assessment of risks, effectiveness of ongoing monitoring, and rate of change within the entity and its environment (GAO-14-704G, 16.06).

[59]OIGs and other oversight entities may conduct evaluations that inform an agency's fraud risk management activities; however, managers themselves are required to monitor and evaluate the agency's internal control system, as described in *Federal Internal Control Standards* (see GAO-14-704G, 16.01–17.06).

[60]In addition to engaging external parties to assist in the actual monitoring and evaluation, managers should also consider monitoring the effectiveness of the internal control systems assigned to such entities, as noted in *Federal Internal Control Standards*. Principle 16 of *Federal Internal Control Standards* notes that management may engage external parties to perform certain operational processes, and managers should consider using ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of the service organization's internal controls over the assigned process.

[61]In GAO, *Designing Evaluations: 2012 Revision (Supersedes PEMD-10.1.4)*, GAO-12-208G (Washington, D.C.: Jan. 31, 2012), we discuss program logic models as a way for managers and evaluators to explain the strategy or logic for achieving the agency's goals. By specifying a theory of program expectations at each step, a logic model or other representation can help evaluators articulate the assumptions and expectations of program managers and stakeholders. At a minimum, the logic model includes performance measures or indicators for staffing and resources (inputs), the type or level of program activities conducted (process), the direct products or services delivered (outputs), or the results of those products and services, such as changes in conditions, behaviors, or attitudes (outcomes).

[62]See the Government Performance and Results Modernization Act of 2010, Pub. L. No. 111-352, 124 Stat. 3866 (2011), which amends the Government Performance and Results Act of 1993, Pub. L. No. 103-62, 107 Stat. 285 (1993).

[63]See GAO-12-208G for additional information on assessing the quality of a prevention or risk management plan.

[64]We have previously reported on the difficulties agencies may face in creating reliable estimates for fraud to serve as baselines for reasons discussed in app. II. For example, see GAO, *Federal Employees Health Benefits Program: Oversight of Carriers' Fraud and Abuse Programs*, GAO-14-39 (Washington, D.C.: Nov. 14, 2013). Also, see GAO-14-704G, 16.02 and 16.03, which says managers can establish a baseline to aid in monitoring and evaluation.

[65]See GAO-14-704G, 16.10 and 17.06.

[66]For instance, participants in GAO's Data Analytics Forum in January 2013 highlighted opportunities for creating feedback loops to aid in resource allocation and managing a high volume of data. One participant said claims deemed suspect are referred for further program or law-enforcement review, or both, and determinations are then fed back into the system. The participant said this feedback loop is designed to allow for constant learning and for the predictive analytics model to be continuously refined to detect fraudulent claims. Another participant stated that the fraud-prevention system her office uses incorporates a continuous feedback loop that refines the way the office prioritizes cases. In addition, senior management takes into account the amount of time that it will take to investigate and resolve cases when deciding where to allocate resources. See GAO-13-680SP.

Appendix I

[67]We did not interview one of the national audit offices; however, it provided written responses to our interview questions. For purposes of this methodology, we counted the written responses as an interview.

[68]Two of the agencies, the Department of Agriculture and the Department of Health and Human Services, were included on both lists. Therefore, we interviewed the OIGs of a total of 8, rather than 10, federal agencies.

[69]GAO, *Federal Grants: Agencies Performed Internal Control Assessments Consistent with Guidance and Are Addressing Internal Control Deficiencies*, GAO-14-539 (Washington, D.C.: July 30, 2014).

[70]Publications included scholarly or peer-reviewed materials, government reports, dissertations, trade publications, conference papers, books, and reports by associations, not-for-profit organizations, and think tanks. In addition, we searched for GAO reports published since January 1, 2009, that referenced GAO's 2006 Fraud Prevention Framework, issued in the following report: GAO, *Individual Disaster Assistance Programs: Framework for Fraud Prevention, Detection, and Prosecution*, GAO-06-954T (Washington, D.C.: July 12, 2006).

[71]Our initial search of databases included publications from January 1, 2009, which resulted in over 200 search results. Given this high volume of documents, we further refined our criteria, in part, by narrowing the time frame of our search criteria.

[72]For instance, see Australian National Audit Office, *Fraud Control in Australian Government Entities: Better Practice Guide* (March 2011); Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework* (New York: American Institute of Certified Public Accountants, 2013); Organisation for Economic Co-operation and Development, *Towards a Sound Integrity Framework: Instruments, Processes, Structures and Conditions for Implementation*, GOV/PGC/GF(2009)1 (Apr. 23, 2009); and Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide* (n.d.).

[73]Content analysis is a methodology for structuring and analyzing written material.

[74]Although the focus groups consisted of multiple individuals, we considered each focus group discussion to be one source for purposes of analyzing practices.

[75]The selection process excluded agencies with negative outlays as well as the Executive Office of the President.

[76]We provided the draft Framework to the Food and Nutrition Service at the Department of Agriculture, as well as the Federal Railroad Administration at the Department of Transportation. Neither agency had comments on the draft Framework.

[77]We requested comments from the Center for Program Integrity (CPI) within the Centers for Medicare & Medicaid Services. CPI did not have comments on the draft Framework.

Appendix II

[78]GAO, *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012). To help ensure that the implementation of FPS was successful in helping the agency meet the goals and objectives of its fraud prevention strategy, we recommended that CMS define quantifiable benefits expected as a result of FPS. In addition, we recommended that CMS describe outcome-based performance targets and milestones that can be measured to gauge improvements to the agency's fraud prevention initiatives attributable to the implementation of FPS. The Department of Health and Human Services concurred with both recommendations.

[79]Fraudulent identity-theft refunds occur when an identity thief uses a legitimate taxpayer's identifying information to file a fraudulent tax return and claims a refund. See GAO, *Identity and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks*, GAO-15-119 (Washington, D.C.: Jan. 20, 2015).

[80]In the report, we noted best practices within the Cost Estimating and Assessment Guide suggest that sensitivity and uncertainty analyses should be used to determine whether assumptions are potentially introducing error into an estimate. For additional information on conducting such analyses, see GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

Appendix III

[81]Data matching is a process in which information from one source is compared with information from another, such as government or third-party databases, to identify any inconsistencies. Data mining analyzes data for relationships that have not previously been discovered. Predictive-analytic technologies include a variety of automated systems and tools that can be used to identify particular types of behavior, including fraud, before transactions are completed.

[82]Data-analytics activities must be implemented consistently with all protections of the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, and other privacy statutes. Specifically, the Computer Matching and Privacy Protection Act requires that federal entities contemplating data matching must (1) protect the privacy of data used in computer matches; (2) complete cost-benefit analyses on all computer matches and report annually on their findings; and (3) establish data integrity boards to approve and review data matches. Pub. L. No. 93-579 (Dec. 31, 1974); 5 U.S.C. 552a, as amended by Pub. L. No. 100-503 (Oct. 18, 1988).

[83]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014), 13.01–13.06. For additional guidance on assessing data reliability, see GAO, *Assessing the Reliability of Computer-Processed Data*, GAO-09-680G (Washington, D.C.: July 2009).

[84]See GAO, *Highlights of a Forum: Data Analytics for Oversight and Law Enforcement*, GAO-13-680SP (Washington, D.C.: July 15, 2013). We established an ongoing community of practice focused on data-sharing challenges. For more information, see: http://www.gao.gov/aac/gds_community_of_practice/overview.

[85]GAO, *Medicare Program Integrity: Greater Prepayment Control Efforts Could Increase Savings and Better Ensure Proper Payment*, GAO-13-102 (Washington, D.C.: Nov. 13, 2012).

[86]GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving, Threat of Refund Fraud*, GAO-14-633 (Washington, D.C.: Aug. 20, 2014).

Appendix VI

[87]The Treasury Do Not Pay Working System was developed to enable federal agencies to reduce improper payments by checking various databases before making payments or awards in order to identify ineligible recipients and prevent fraud or errors from being made. Through the Do Not Pay initiative, agencies can use the Social Security Administration's Death Master File (public version), Treasury Offset Program Debt Check, Department of Health and Human Service's List of Excluded Individuals and Entities, and General Services Administration's System for Award Management Exclusion Records, among other data sources, to assist in verifying eligibility. This effort was first required by a Presidential Memorandum issued on June 18, 2010, and was established in law as the Do Not Pay Initiative, by the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), Pub. L. No. 112-248 (Jan. 10, 2013).

[88]GAO-13-680SP.

[89]The Federal Acquisition Regulation (FAR) requires certain contractors to implement an ongoing business ethics awareness and compliance program that includes conducting training and otherwise disseminating information appropriate to an individual's respective roles and responsibilities. The FAR requires that this training be provided to the contractor's employees, and as appropriate, the contractor's agency and subcontractors. (48 C.F.R. § 52.203-13).

[90]GAO, *Medicare Program Integrity: Expanded Federal Role Presents Challenges to and Opportunities for Assisting States*, GAO-12-288T (Washington, D.C.: Dec. 7, 2011).

[91]GAO, *Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers*, GAO-11-721T (Washington, D.C.: June 2, 2011).

Appendix IV

[92]Pursuant to an amendment made to IPIA by section 4 of IPERIA, for fiscal year 2014, the threshold is potential improper payments exceeding (1) both 1.5 percent of program outlays and $10 million or (2) $100 million regardless of the percentage.

[93]Risk factors one through seven are discussed in IPERA, Pub. L. No. 111-204 (July 22, 2010), and codified as amended at 31 U.S.C. § 3321 note. The Office of Management and Budget (OMB) has since issued updated guidance, applicable beginning with fiscal year 2014 reporting. This guidance—OMB Memorandum No. M-15-02, app. C to Circular No. A-123, *Requirements for Effective Estimation and Remediation of Improper Payments* (Oct. 20, 2014)—includes factors 8 and 9 of this list.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact:
Stephen M. Lord, (202) 512-6722 or LordS@gao.gov

Staff Acknowledgments:
In addition to the contact named above, Linda Miller (Assistant Director), Gavin Ugale (Analyst-in-Charge), Erin McLaughlin, Maria McMullen, and Steven Putansu made key contributions to this publication. Also contributing to this publication were Tracy Abdo, Seto Bagdoyan, Gary Bianchi, Marcus Corbin, Beryl Davis, Leia Dickerson, Julia DiPonio, Colin Fallon, Holly Halifax, Robert Heilman, Lauren Kirkpatrick, Kristen Kociolek, Barbara Lewis, Jessica Lucas-Judy, Flavio Martinez, Marc Molino, Philip Reiff, Brynn Rovito, Alexandra Stone, Matthew Valenta, and April Van Cleef.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimonies

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

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

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE