U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Combating Fraud: Approaches to Evaluate Effectiveness and Demonstrate Integrity

Accessible Version

January 2026

GAO-26-107609

Contents

Introduction 1
Why GAO Developed This Technical Appendix 2
How GAO Developed This Technical Appendix 3

Technical Appendix 4
Guide to Reading the Technical Appendix 5
1. Commit to Combating Fraud by Creating an Organizational Culture and Structure Conducive to Fraud Risk Management 6
2. Plan Regular Fraud Risk Assessments and Assess Risks to Determine a Fraud Risk Profile 8
3. Design and Implement a Strategy with Specific Control Activities to Mitigate Assessed Fraud Risks and Collaborate to Help Ensure Effective Implementation 11

Endnotes 18

GAO Contact and Staff Acknowledgments 20

Figures

Figure 1: The Fraud Risk Management Framework 1
Figure 2: Incorporating Feedback to Continually Adapt Fraud Risk Management Activities 2
Figure 3: Sample of Illustrative Comments from GAO's Survey of Employees at the Export-Import Bank of the United States 7
Figure 4: Evaluating the Effectiveness of Artificial Intelligence (AI) Systems 10
Figure 5: Estimating the Financial Value of Preventing Ongoing Identity Compromise 15
Figure 6: Hypothetical Example of Cost Savings Information 16
Figure 7: Final Consideration: Avoid Perverse Incentives 17

Abbreviations

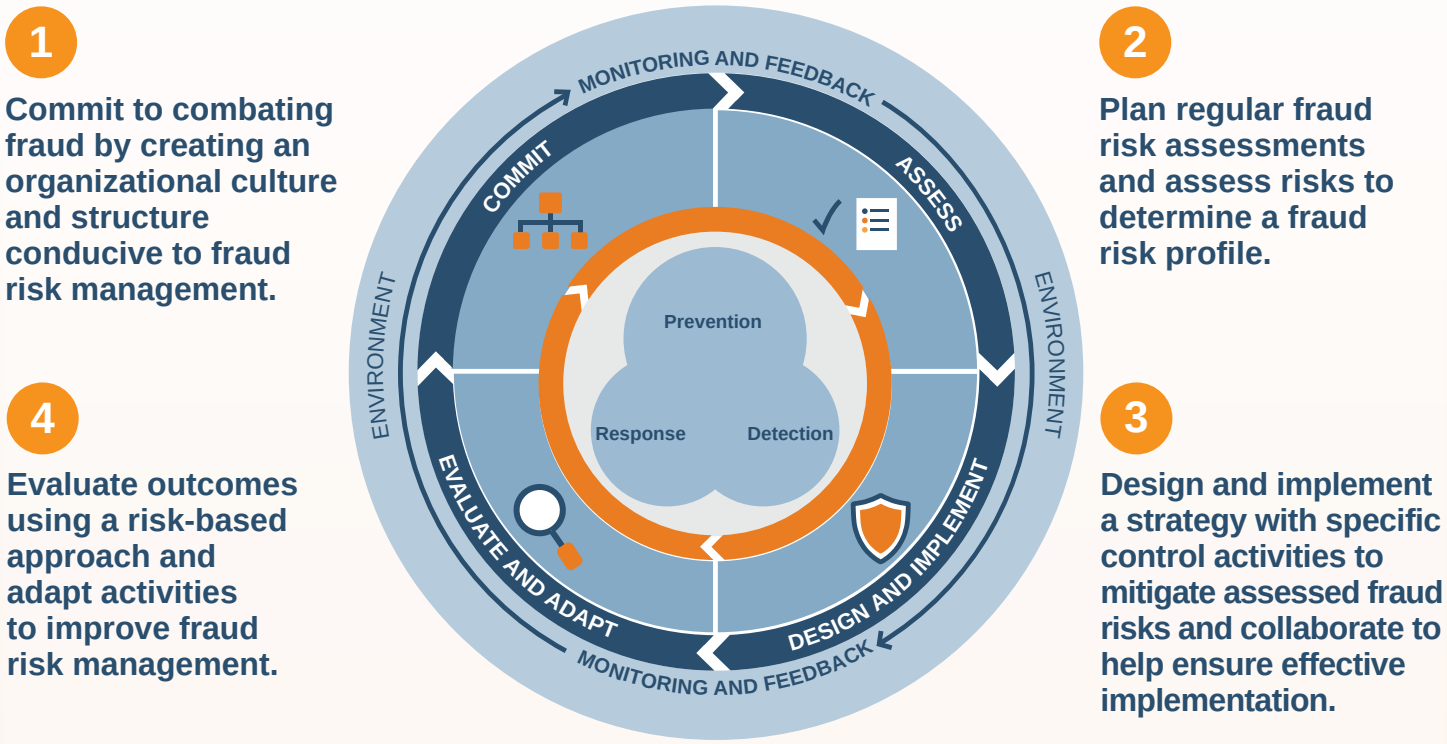
AI	artificial intelligence
CMS	Centers for Medicare & Medicaid Services
COVID-19	coronavirus disease
Evidence Act	Foundations for Evidence-Based Policymaking Act of 2018
EXIM	Export-Import Bank of the United States
Fraud Risk Framework	*A Framework for Managing Fraud Risks in Federal Programs*
HFPP	Healthcare Fraud Prevention Partnership
HHS	Department of Health and Human Services
IRS	Internal Revenue Service
OIG	Office of Inspector General
OMB	Office of Management and Budget
PBGC	Pension Benefit Guaranty Corporation
PSFA	United Kingdom's Public Sector Fraud Authority
ROI	return on investment
SSA	Social Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

Introduction

Demonstrating strong internal controls and program integrity is important to protect taxpayer dollars and maintain public trust. Fraud risk management is essential for protecting program integrity by continuously and strategically mitigating the likelihood and impact of fraud.[1] This document serves as a technical appendix to GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). The framework was issued in 2015 and provides a comprehensive set of leading practices, organized into four components, for agency managers to use when developing or enhancing efforts to combat fraud in a strategic, risk-based manner (see fig. 1).[2]

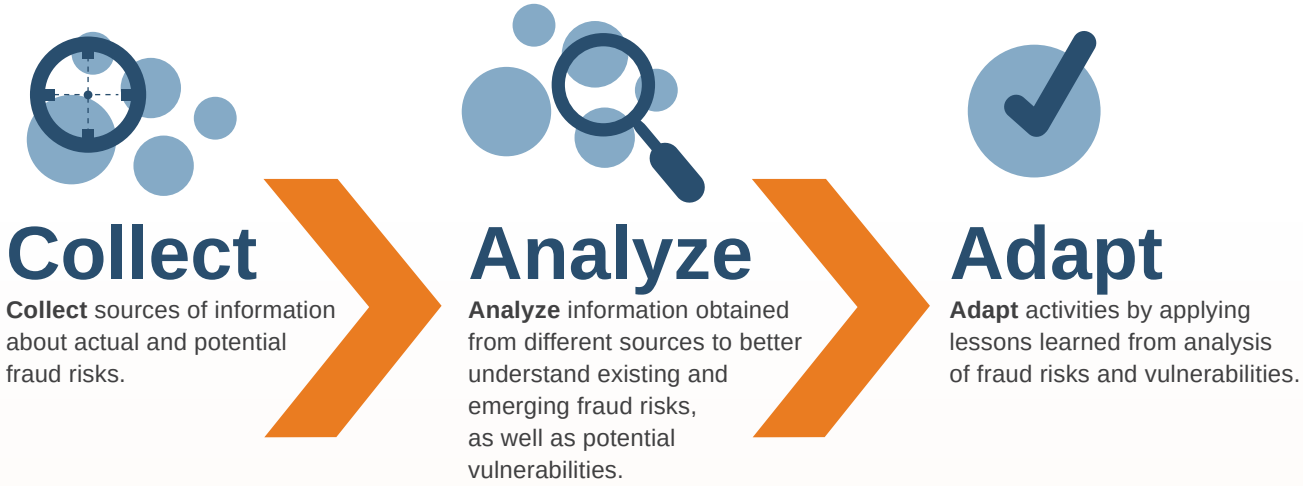
Figure 1: The Fraud Risk Management Framework



Source: GAO. | GAO-26-107609

All federal programs and operations are at risk of fraud, and managers maintain the primary responsibility for enhancing program integrity. Component 4 of the Fraud Risk Framework directs program managers to evaluate outcomes using a risk-based approach and adapt fraud risk management activities from the first three components to improve fraud risk management (see fig. 2). Additionally, the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act) directs agencies to use evidence, such as that developed through evaluations, to aid policymaking.[3] Both GAO and the Office of Management and Budget (OMB) provide guidance or tools that program managers can use to carry out these evaluations.[4]

Figure 2: Incorporating Feedback to Continually Adapt Fraud Risk Management Activities



Source: GAO. | GAO-26-107609

Agencies, Offices of Inspector General (OIG), GAO, and others have identified and reported significant actual or potential financial savings due to fraud risk management activities. Examples include the following:

- The Department of the Treasury reported saving over $4 billion in fraud and improper payments in fiscal year 2024 using enhanced controls, such as improved data analytics.[5]
- The Pandemic Response Accountability Committee used statistical sampling to estimate that data analytics could have prevented over $79 billion in potentially fraudulent COVID-19 program payments.[6]
- GAO estimated that the Small Business Administration's use of additional antifraud safeguards in the Paycheck Protection Program and other COVID-19 programs resulted in more than $12 billion in savings as of the end of fiscal year 2023.[7]
- The United Kingdom's Public Sector Fraud Authority's review of workforce and fraud loss data determined that preventative antifraud activities delivered a return on investment around four times that of reactive enforcement and compliance activity.[8]

Agencies have also demonstrated the ability of fraud risk management activities to reduce nonfinancial losses due to fraud. Nonfinancial losses may not pose a direct financial cost but can lead to other potentially harmful outcomes. For example, in 2023, GAO reported that improved security screening of researchers could help prevent the fraudulent acquisition and use of sensitive U.S. research and technology.[9]

Why GAO Developed This Technical Appendix

Evaluations can help agencies show the value of their fraud risk management activities.[10] Program managers also need to understand the effectiveness of their fraud risk management activities so they can adjust their efforts to better protect their resources against fraud.

Component 4 of GAO's Fraud Risk Framework describes how agencies can use robust evaluations that are comprehensive in scope, incorporate a range of metrics and outputs beyond financial returns, and use input from stakeholders to better understand program outcomes. While agencies may have varying levels of resources, program managers can tailor evaluations to align with available capacity and the specific activities being assessed.

However, our work has shown that agencies face challenges in effectively implementing leading practices in the Fraud Risk Framework, in particular Component 4. For example, in 2023, we found that of the 24 federal agencies we surveyed,

- one-third did not have regular ongoing monitoring or evaluation activities, and
- one-half did not regularly make changes based on evaluation results.[11]

Agencies continue to face these challenges, despite requirements to use the Fraud Risk Framework's leading practices to manage fraud risks.[12] To assist program managers with implementing Component 4 of the Fraud Risk Framework, we developed this technical appendix, which supplements and complements the Framework. Specifically, we identified examples, methods, and considerations that can be used to help evaluate the effectiveness of and adapt fraud risk management activities within Components 1, 2, and 3 of the Fraud Risk Framework.

How GAO Developed This Technical Appendix

As with the Fraud Risk Framework, we solicited a wide range of views when developing this appendix. We collected information from interviews, written questionnaires, and relevant literature. We then analyzed this information and identified examples of fraud risk management evaluation activities, as well as relevant considerations.

We contacted individual federal agencies, the Chief Financial Officers Council, Small Agency Council, and Council of the Inspectors General on Integrity and Efficiency to identify agencies and OIGs to interview. We also contacted selected external entities, based on our review of their relevant publications and expertise in antifraud activities.

We gathered information on evaluation activities from agencies and OIGs. While program managers, rather than OIGs, are responsible for implementing the Fraud Risk Framework and conducting fraud risk management activities, program managers can learn from OIGs' valuable insights and actions.

We interviewed officials from 31 entities with antifraud evaluation experience across sectors, including officials with 11 federal agencies, eight OIGs, and the Pandemic Response Accountability Committee. We also interviewed antifraud experts from 11 external entities, including the World Bank, the United Kingdom's Public Sector Fraud Authority, the Association of Certified Fraud Examiners, the Institute of Internal Auditors, and academia. We selected agencies, OIGs, and external entities based on our understanding of their evaluative activities and knowledge. We interviewed these officials to collect information on their organizations' efforts to evaluate the effectiveness of fraud risk management activities.

We reviewed relevant literature to identify examples of (1) approaches to evaluate fraud risk management activities and (2) considerations for managers to keep in mind when performing these evaluations. We reviewed existing frameworks and guides related to fraud risk management and integrity, including publications by the International Public Sector Fraud Forum, the Institute of Internal Auditors, the Association of Certified Fraud Examiners, and federal agencies, among others. We also reviewed the Evidence Act and associated OMB guidance.[13]

We compiled a list of approaches that entities reported using to evaluate their fraud risk management activities. We captured these methods from written responses, interviews, or our review of relevant reports and literature. We selected approaches for evaluating fraud risk management activities that could be achieved by programs with varying resources, as well as examples where agencies may have used these approaches. Given the scope of this work, we do not provide an exhaustive list of approaches.

Source: lovemask/stock.adobe.com (icons). | GAO-26-107609

We provided a draft of the technical appendix to select antifraud entities for their review and input. Specifically, we requested that reviewers comment on the relevancy and completeness of our selected approaches and examples, and we incorporated their comments, as applicable.

To obtain additional insights to improve the usability of this technical appendix, we provided a full draft for comments and consideration to the national audit offices of Australia, Canada, and the United Kingdom, as well as other organizations, including the United Kingdom's Public Sector Fraud Authority, Service Canada, the Canada Revenue Agency, the Australia Commonwealth Fraud Prevention Centre, the Pandemic Response Accountability Committee, the Association of Certified Fraud Examiners, and the Institute of Internal Auditors.

We also provided a draft of the appendix for technical comments to

- OMB;
- the Departments of Health and Human Services' Centers for Medicare & Medicaid Services and the Treasury, including the Internal Revenue Service and the Bureau of the Fiscal Service, the Social Security Administration, and the National Labor Relations Board; and
- the OIGs for the Department of Health and Human Services, the Internal Revenue Service, and the Pension Benefit Guaranty Corporation.

We incorporated those technical comments we received, as appropriate.

We conducted our work from May 2024 to January 2026 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.

Technical Appendix

This technical appendix to GAO's Fraud Risk Framework describes evaluation approaches for fraud risk management activities. The Fraud Risk Framework consists of the following four components for effectively managing fraud risks:

- Component 1 - Commit,
- Component 2 - Assess,
- Component 3 - Design and Implement, and
- Component 4 - Evaluate and Adapt.

These approaches can be modified to fit the circumstances and conditions relevant to different programs and activities. While the primary target audience is managers in the U.S. federal government, the approaches may also be applicable to state, local, and foreign government agencies, as well as nonprofit entities that are responsible for fraud risk management.

This appendix focuses on implementing **Component 4** of the Fraud Risk Framework: Evaluate Outcomes Using a Risk-Based Approach and Adapt Activities to Improve Fraud Risk Management.

It highlights approaches managers have used—or could use—to evaluate and adapt fraud risk management activities across **Components 1, 2, and 3.**

Source: GAO. | GAO-26-107609

The illustrative examples in the technical appendix are not the only methods or options to evaluate the effectiveness of a program's fraud risk management approach. Each program should implement Component 4 of the Fraud Risk Framework considering its unique fraud risk environment. Citing a program-specific example does not indicate that the referenced program's fraud risk management activities fully align with leading practices.

Guide to Reading the Technical Appendix

Component number

Component name

We use signposts to signify the applicable component, such as this signpost for Component 1.

1 Fraud Risk Framework Component

Below each component name, we include subheaders for each of the Fraud Risk Framework's overarching concepts. We also include evaluation approaches and examples, as well as benefits. Each overarching concept provides relevant evaluation approaches and examples, as well as benefits. Benefits include things such as potential improvements to fraud risk management. Our examples include references to **outputs**, which are the direct products or services delivered, such as the number of trainings provided. The examples also include references to **outcomes**, which are the results derived from those products and services, such as an increase in fraud prevention attributed to trainings. The "consider this" section provides suggestions for program managers to improve their evaluations and may be applicable to multiple approaches.

Fraud Risk Framework Overarching Concept	
Evaluation approach and example	**Benefit**
Evaluation approach summary. A further explanation and example of an evaluation approach that program managers could take to assess the relevant overarching concept.	*The potential beneficial impact of the evaluation approach on a program.*

Consider this...

- Considerations for managers to keep in mind when performing evaluations.

For each Fraud Risk Framework component, we also provide at least one selected in-depth example that further describes an evaluation approach, including the methodology used and evaluation performed.

Example: Selected in-depth example summary
In-depth explanation of selected example.

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

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

Evaluation approach and example	Benefit
Analyze employee survey responses. Managers can use survey responses to evaluate employees' perspectives on fraud risk management efforts. For example, GAO surveyed a wide range of employees of the Export-Import Bank of the United States (EXIM) and analyzed the responses.[14] As part of the analysis, GAO identified and examined perceived differences between management and nonmanagement staff regarding organizational culture and attitudes toward fraud and fraud risk management. Survey results indicated that perceptions varied about the antifraud tone set by senior management, as well as by nonsenior management (*see in-depth description in example 1*).	*Survey responses can help organizations assess strengths and gaps in the agency's antifraud culture across all staff levels and serve as baseline data for future culture interventions.* *For example, to understand and address divergent views indicated in GAO's survey, as well as promote and sustain an antifraud tone, EXIM provided additional trainings, conducted an internal survey, and designated a team to enhance communication and oversight.*
Analyze text and generate insights. Managers can use natural language processing to analyze large amounts of free form text, including internal written communications such as management memorandums or employee training evaluations. For example, natural language processing models can scan, synthesize, and summarize meeting transcripts and training feedback to detect patterns in employee sentiment, concerns with leadership, or insider fraud threats.[15]	*Natural language processing can produce insights about an agency's culture, such as employees' perceptions of leadership, which can help managers proactively shape an agency's culture. Analysis may also identify hidden or unrealized concerns that may not be able to be identified through other means, such as agency surveys.*

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

Evaluation approach and example	Benefit
Analyze documentation and compare against leading practices. Managers can analyze documentation to assess adherence to leading fraud risk management practices. For example, reviewing organizational charts and standard operating procedures can provide insights into whether a program's designated entity has the necessary responsibilities and authorities to design and oversee fraud risk management activities.	*Assessing documentation can help managers evaluate whether their organization has a dedicated entity that aligns with fraud risk management leading practices and assess whether gaps exist.*
Analyze training metrics and track results over time. Managers responsible for leading fraud risk management trainings can measure outputs and outcomes to assess their efficacy. For example, an output could include the number of trainings provided. An outcome could include the change in the number of reported potential fraud instances before and after the training.	*Tracking metrics, including both outputs and outcomes associated with specific fraud risk management activities, can help leadership identify areas to improve.*

Consider this...

- Culture is intangible and can be challenging to measure, but it is still possible and important to take its measure.
- Measuring and assessing culture can provide information to help managers drive change.
- Evaluating how much an organization invests in fraud risk management can help assess leadership commitment.
- External sources, such as whistleblower reports and stakeholder feedback, can provide insights into organizational culture.

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

In-Depth Example 1 of Evaluation Approach

Example 1: Analyze employee survey responses to understand their perceptions of organizational antifraud commitment

The Export-Import Bank of the United States (EXIM) is a wholly owned government corporation that serves as the nation's export credit agency. In 2018, GAO surveyed all nonsenior management EXIM employees to examine the extent to which EXIM had established an organizational culture and structure conducive to fraud risk management. The survey enabled GAO to assess perceptions of organizational culture and attitudes toward fraud and fraud risk management and whether employees viewed senior management as committed to establishing and maintaining an antifraud culture.

Methodology

The survey

- included closed- and open-ended questions on management's actions, fraud-related training and information, the antifraud environment, and employees' personal experiences with fraud;
- used recognized survey design practices in collecting, processing, and analyzing the survey data; and
- sought to obtain a range of different employees' views.

Findings

GAO found that EXIM managers and staff generally held positive views of EXIM's antifraud culture but that EXIM had opportunities to improve. For example, a significant portion of EXIM staff raised concerns about potentially competing objectives regarding timeliness. While EXIM staff needed sufficient time to perform due diligence activities to prevent and detect fraud prior to approving transactions, staff also needed to process transactions in a timely manner to meet customer needs and achieve EXIM's mission. Figure 3 provides illustrative comments showing opportunities for EXIM to further set an antifraud tone.

Figure 3: Sample of Illustrative Comments from GAO's Survey of Employees at the Export-Import Bank of the United States

"More due diligence should be required in order to qualify for the U.S. government's support."

"A more proactive approach to fraud detection, rather than a reactive approach, would be more prudent. This means trying to sniff out fraud [at] the preapplication and underwriting stages."

"The Bank is more concerned with increasing sales than preventing fraud."

Source: GAO. | GAO-26-107609

Results

As a result of GAO's review, EXIM implemented methods to further promote and sustain an antifraud tone across its organizational culture. For example, it established ongoing fraud risk training for all employees and documented fraud risk management roles and responsibilities for all levels of the agency.

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

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

Evaluation approach and example	Benefit
Evaluate fraud risk assessment processes. Managers can evaluate program processes to effectively identify and assess fraud risks. This evaluation can include comparing whether observed fraud aligns with what was identified during the risk assessment process. For example, the National Labor Relations Board developed a tool to evaluate its fraud risk management processes, including those for planning and developing risk assessments. The tool describes specific control activities and test plans, such as reviews of procedures and internal controls. The tool also supports gap analysis to identify potential deficiencies and recommend corrective actions.	*Periodically evaluating a program's approach to identifying fraud risks can ensure a robust assessment process that identifies and adapts to emerging risks.*
Evaluate stakeholder involvement in the fraud risk assessment process. Managers can evaluate internal fraud risk assessment processes to ensure adherence to leading practices, such as the practice to involve relevant stakeholders. For example, managers can determine if important stakeholders, such as the OIG, were included when developing their risk assessments, to help identify fraud risks.	*Ensuring that the fraud risk assessment follows leading practices can help identify risks and appropriately tailor resources and control activities, which can enhance its effectiveness.*

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

Evaluation approach and example	Benefit
Establish a continuous feedback loop to track, monitor, and reassess fraud risks. Managers can establish a process to continually reassess program fraud risks. For example, the Social Security Administration (SSA) continually reassesses its fraud risks and updates its fraud risk profile to better understand and respond to emerging threats (*see in-depth description in example 2*).	*Tracking, monitoring, and reassessing fraud risks can help address internal control vulnerabilities.*
Use technology to improve a program's fraud risk profile. Managers can leverage artificial intelligence (AI) to identify emerging fraud risks or fraud schemes outside their knowledge base. For example, AI systems can analyze documents, such as program guidance and information on known fraud schemes, to simulate how bad actors might exploit agency programs. Managers can use these results to identify internal gaps in controls and strengthen their fraud risk profiles.[16] Further, managers should evaluate the effectiveness of the AI systems used for fraud risk management activities (see fig. 4 on evaluating the effectiveness of AI systems).	*Technology such as AI can help identify risks that may not have been previously identified. Assessing the accuracy, quality, and completeness of the generated information ensures that fraud risk management activities are reliable and effective at fighting fraud.*

Consider this...

- Risk assessments can be open to manipulation, such as when funding or staff pay are tied to fraud reduction targets. This may lead to over- or understated fraud risks to meet targets. Managers should avoid perverse incentives when assessing fraud risks by carefully setting performance targets (see fig. 7 for further discussion of perverse incentives).
- As agencies start identifying and tracking fraud, they will likely find more of it, which means they may have to adapt their risk assessments midanalysis to reflect new information.
- Consider both financial and nonfinancial fraud when evaluating risk assessments.
- Identifying fraud should be seen as a good thing that helps lead to proactive actions to prevent and combat it.

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

In-Depth Example 2 of Evaluation Approach

Example 2: Continuously reassess fraud risks and associated antifraud activities

According to SSA officials, SSA continuously reassesses its fraud risks and the effectiveness of associated antifraud activities. After initially identifying its fraud risks, SSA develops a fraud risk profile, which informs the control activities to be designed and implemented. SSA then collaborates with agency stakeholders to implement antifraud activities to address fraud risks. Specifically, SSA

- requests regular quarterly updates from stakeholders to track the progress of each antifraud activity,
- takes immediate action if staff detect changes in the likelihood or impact of existing fraud risks,
- assesses the effectiveness of antifraud activities,
- revises ineffective or infeasible activities through coordination with stakeholders, and
- updates its risk profiles with revised fraud risks and continues the reassessment process.

In one example, SSA's data analytics team flagged suspicious transactions due to changes in beneficiaries' direct deposit information. Based on a review of the transactions, SSA determined that some controls were ineffective in preventing fraudsters from redirecting beneficiaries' direct deposits. As a result, SSA updated its policies and procedures to mitigate the risk to an acceptable level.

Fraud Risk Profile

A Framework for Managing Fraud Risks in Federal Programs notes that a fraud risk profile forms the basis of a program's antifraud strategy and includes information such as

- the identified fraud risk;
- fraud risk factors;
- fraud risk owner;
- inherent risk likelihood, impact, and significance;
- fraud risk tolerance;
- existing antifraud controls;
- residual risk likelihood, impact, and significance; and
- the fraud risk response.

Source: GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). | GAO-26-107609

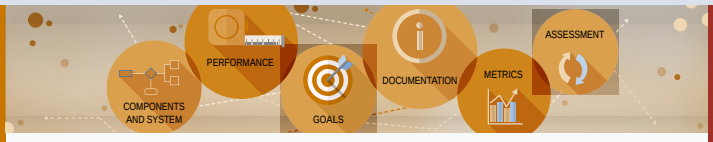
Source: icons-studio/stock.adobe.com (icons).

Figure 4: Evaluating the Effectiveness of Artificial Intelligence (AI) Systems

We have previously reported that AI systems can provide opportunities for improved government operations and fraud detection. For example, machine learning algorithms, which identify statistical relationships between inputs and outputs from training datasets, might improve prevention or detection of fraud by quickly revealing anomalous patterns, behaviors, and relationships. However, AI systems pose unique challenges for independent assessments and audits to promote accountability because their inputs and operations are not visible to the user. Such systems can be an opaque "black box," either because the inner workings of the software are inherently very difficult to understand, or because vendors do not reveal them for proprietary reasons. This lack of transparency limits the ability of auditors and others to detect error or misuse.

As with other fraud risk management activities described in this technical appendix and the Fraud Risk Framework, AI systems should be evaluated to determine if they are functioning effectively and achieving their intended objectives. GAO's AI Accountability Framework identifies key accountability practices—centered around the principles of governance, data, performance, and monitoring—to help federal agencies and others use AI responsibly. Performance and monitoring principles described in the graphic below can be used to evaluate the effectiveness of AI systems utilized to combat fraud by ensuring these systems produce results that are consistent with program objectives and by monitoring systems for relevance and reliability over time.

Performance



Key Practices

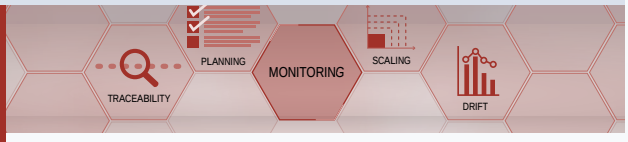
Performance at the Component Level

- **Documentation:** Catalog model and non-model components, along with operating specifications and parameters.
- **Metrics:** Define performance metrics that are precise, consistent, and reproducible.
- **Assessment:** Assess the performance of each component against defined metrics to ensure it functions as intended and is consistent with program goals and objectives.
- **Outputs:** Assess whether outputs of each component are appropriate for the operational context of the AI system.

Performance at the System-Level

- **Documentation:** Document the methods for assessment, performance metrics, and outcomes of the AI system to provide transparency over its performance.
- **Metrics:** Define performance metrics that are precise, consistent, and reproducible.
- **Assessment:** Assess performance against defined metrics to ensure the AI system functions as intended and is sufficiently robust.
- **Bias:** Identify potential biases, inequities, and other societal concerns resulting from the AI system.
- **Human supervision:** Define and develop procedures for human supervision of the AI system to ensure accountability.

Monitoring



Key Practices

Continuous Monitoring of Performance

- **Planning:** Develop plans for continuous or routine monitoring of the AI system to ensure it performs as intended.
- **Drift:** Establish the range of data and model drift that is acceptable to ensure the AI system produces desired results.
- **Traceability:** Document results of monitoring activities and any corrective actions taken to promote traceability and transparency.

Assessing Sustainment and Expanded Use

- **Ongoing assessment:** Assess the utility of the AI system to ensure its relevance to the current context.
- **Scaling:** Identify conditions, if any, under which the AI system may be scaled or expanded beyond its current use.

Notes: For reference, see the following GAO reports: GAO, *Fraud and Improper Payments: Data Quality and a Skilled Workforce Are Essential for Unlocking the Benefits of Artificial Intelligence*, GAO-25-108412 (Washington, D.C.: Apr. 9, 2025); and *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, GAO-21-519SP (Washington, D.C.: June 2021). Also, the figure refers to both the component level and the system level. Components are technology assets that represent building blocks of an AI system, while a system is the integrated whole.

Sources: GAO; treenabeena/stock.adobe.com (header). | GAO-26-107609

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

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

Evaluation approach and example	Benefit
Assess documentation to evaluate an antifraud strategy against leading practices. Managers can compare their fraud risk management documentation with leading practices to identify gaps and implement changes, as needed. For example, a program can review its antifraud strategy by assessing whether it addresses all risks identified by a fraud risk assessment and includes mechanisms to monitor progress on corrective actions.	*Assessing documentation can help ensure that antifraud strategies are targeted, actionable, and effectively manage fraud risk.*

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

Evaluation approach and example	Benefit
Assess the effectiveness of internal controls. Managers can assess and evaluate the effectiveness of their internal controls to ensure they are working as intended and adjust as needed. For example, these assessments can be targeted to quickly determine the effectiveness of a single control. Additionally, an organization can test specific vulnerabilities to a payment system designed to verify recipient eligibility and then use this information to address the vulnerability. These assessments can also include comprehensive testing of multiple controls to determine the effectiveness of the overall control environment.[17] For example, the Internal Revenue Service (IRS) reviews the filters it uses to screen for identity theft and modifies or retires models with high false positives.	*Assessing internal controls can provide managers with assurance that they are operating effectively to address fraud risks.* *Between tax processing years 2020 and 2021, the IRS updated its filters based on emerging identity theft schemes. These changes helped the IRS identify over 41,000 refunds at risk of identity theft and protected $2.3 trillion in tax refund returns.*[18]
Benchmark antifraud program performance against metrics. Managers can develop and use metrics or key performance indicators to understand the effectiveness of their antifraud program's performance as compared with past performance, expectations, and relevant peers. For example, managers can track indicators over time, such as the number of suspicious payments prevented, the number of referrals, the number of substantiated cases, and the average or median losses per identified fraud incident.	*Developing and measuring performance against multiple benchmarks can help managers evaluate and adapt specific or overall antifraud activities.*
Compare costs and benefits. Managers can assess and compare the costs and benefits of their programs' antifraud investments. For example, to determine the impact of a new identity fraud training and controls, managers could estimate the value at risk and the probability of identity fraud with and without the new training and controls. They can then assess those savings against the cost of the program. Managers can also calculate return on investment (ROI), or the financial return for every dollar in antifraud investments (*see in-depth description in example 3*).	*Comparing costs and benefits for fraud controls can help a program demonstrate its value, justify funding decisions, and prioritize resource allocation.* *For example, the IRS estimated that sustained investments to improve service, increase filings and compliance, and reduce fraud would yield up to $497 billion in additional revenue during fiscal years 2024-2034.*

Cost-benefit calculations can also include indirect benefits. For example, the IRS developed a methodology to estimate the expected additional tax revenues resulting from staffing changes and technology improvements. The methodology captured some of the indirect benefits of enhanced compliance, such as through deterrence.[19]	
Calculate cost savings from using data analytics to identify fraud. Managers can calculate the cost savings of their data analytics efforts to help demonstrate their efficacy, but also to help inform improvements to their systems. For example, the Pension Benefit Guaranty Corporation (PBGC) OIG used data analytics to compare multiple data sources to identify deceased individuals on payroll. The OIG removed these individuals from the PBGC's list of payees and calculated the savings associated with prevented improper or fraudulent payments by multiplying the pension payment amount for the individuals by the number of months the individual was paid postdeath.[20]	*Quantifying cost savings from fraud analytics can help demonstrate measurable returns and strengthens the case for using analytic tools.* *For example, the PBGC OIG identified 56 deceased participants and $1.1 million in improper or fraudulent payments, with a value of discontinued future benefit payments of $479,000.*
Calculate cost savings due to fraud prevention. Cost savings estimates of fraud risk management activities can include the effects of prevention, in addition to savings from detection and recoveries. Fraud prevention can occur when enforcement, such as legal action, deters a population of bad actors from committing further fraud. For example, the Healthcare Fraud Prevention Partnership (HFPP), overseen by the Centers for Medicare & Medicaid Services (CMS), published guidance for measuring fraud prevention savings.[21] The guidance stated that these savings can outweigh those of recoveries but are more difficult to measure. It recommends comparing preenforcement and postenforcement costs to estimate the savings. (*See in-depth description in example 4.*)	*Fraud prevention, including deterrence, decreases the need to chase after and recover stolen funds. Demonstrating the value of fraud prevention can help inform antifraud resource allocation decisions.* *For example, according to HFPP, a whistleblower lawsuit resulted in $275 million in recoveries, as well as between $2.6 billion and $5.9 billion in savings from deterred fraud.*[22]
Validate reporting methodologies with a third party. Managers can coordinate with stakeholders or third-party entities to evaluate and validate their fraud risk reporting methods and incorporate necessary changes to their plan. For example, through its mandate, the United Kingdom's Public Sector Fraud Authority (PSFA) requires that public bodies calculate and report the number and value of detected, prevented, and recovered fraudulent payments each quarter. The PSFA then convenes an expert panel to assess whether public bodies have correctly calculated financial benefits and applied the appropriate methodology to the evaluation. Additionally, the Department of Health and Human Services' (HHS) OIG analyzed the methodologies used to calculate a return on the agency's Fraud Prevention System, a large-scale investment. Findings included that more granular data and better tracking would improve calculations of actual and projected savings from preventing Medicare fraud.[23]	*Third-party confirmation of reporting methods and calculations increases accuracy, ensures objectivity, and helps standardize data across entities. Robustly evaluating significant fraud risk investments can justify its expense while also producing information that can be used to enhance effectiveness.*
Covertly test internal controls to assess efficacy of internal control systems. Managers can covertly use or simulate known fraudster methods to determine if their internal controls are working as intended and evaluate their ability to detect fraud. For example, managers can fabricate invoices that contain errors or exceed a certain threshold and monitor whether the invoices are flagged, rejected, or approved. Managers can then use the results to adjust internal controls, as needed.[24]	*Covert testing and simulations can expose real-world weaknesses in internal controls, helping programs identify vulnerabilities, tighten safeguards, and strengthen overall risk posture.*

Estimate the deterrence effect of antifraud controls. Managers may consider using the literature in their field and the historical data from their program to understand the potential impact of their antifraud controls. For example, the IRS used academic literature and historical data to quantify the deterrence effects of audits on select taxpayers. Taxpayer audits can detect noncompliance and deter future noncompliance because fraudsters may be more cautious as the perceived possibility of being caught increases.[25]	*Estimating deterrence helps gauge the broader impact of audits on preventing fraud. This can help managers allocate audit resources and more fully quantify the value of fraud risk management.* *For example, the IRS estimated that sustained investments in audits of certain taxpayers could result in an additional $38.8 billion in revenue collected for fiscal years 2024-2034 due to specific deterrence effects.*

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

Evaluation approach and example	Benefit
Assess responses to past incidents of fraud. Managers can evaluate their responses to past incidents of fraud. For example, managers can assess the timeliness and disposition of their referrals of potential fraud to the OIG to determine if their processes are working as intended. Managers can also analyze specific fraud-related case studies to identify ways to improve their response to fraud.	*Evaluating past experiences, including referrals, can help managers improve their responses to identified fraud in the future.*
Calculate cost savings from a fraud response plan. Cost savings estimates from a program's plan to respond to fraud can help managers determine the value of the plan and identify necessary adjustments for how the program will respond to future instances of identified fraud. Different points to calculate savings from fraud response plans include: • where the fraud was detected (point of interdiction); • where the fraud would have continued to result in loss, had it not been caught (future loss prevented); and • process changes based on detected fraud that prevented subsequent fraud (upstream prevention).[26] For example, managers can calculate preventative savings when a payment has been stopped from being processed due to the detection of suspected fraud through an internal control.	*Calculating savings from a response plan shows the value of strong controls by quantifying losses avoided – both immediate and future – and emphasizes the importance of proactive fraud risk management.*
Use referral feedback to evaluate and improve fraud response. Managers can review feedback on fraud referral processes and incorporate necessary changes to improve future fraud response. For example, IRS civil fraud staff solicit feedback on internal fraud referrals made to the IRS' criminal fraud division. This feedback helps foster continual improvement in the quality and sustainability of the fraud referral process and enhances intra-agency coordination. Similarly, CMS monitors the volume of staff referrals to law enforcement to evaluate how effectively its coordination program fosters collaboration among agency personnel, contractors, law enforcement, and OIGs.	*Collecting and analyzing qualitative and quantitative information can improve referral processes and build stronger enforcement partnerships.* *For example, according to CMS, within 1 year of coordinating meetings focused on collaboration, Medicare referrals to law enforcement increased by more than 200 percent.*[27]

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

Evaluation approach and example	Benefit
Evaluate working relationships with stakeholders. Managers can gather, assess, and utilize internal and external stakeholder feedback to build reciprocal working relationships, such as with OIGs. For example, managers can work with communities of practice to facilitate peer learning about fraud risk management and antifraud strategies. Additionally, the HHS OIG looked holistically at improving efficiency and effectiveness in delivering publicly available resources and created a feedback mechanism with the public. This included a request for information that sought public input on OIG resources and how the OIG can enhance usefulness and timeliness and improve accessibility and usability of their resources.[28]	*Implementing a stakeholder feedback loop helps improve communication and collaboration and can lead to stronger partnerships and more effective fraud prevention strategies.*

Consider this...

- Focus on measuring outcomes versus outputs.
- Identify and use metrics relevant to your program goals.
- Reviewing program documentation, such as procedures, can be helpful but should be supplemented with additional evaluation activities, such as internal control assessments.
- Determining the savings from fraud risk management, such as calculating ROI, can be difficult but demonstrates the value of fraud risk management activities and investments.
- Seek to determine cost savings holistically, including direct and indirect costs and benefits, as well as financial and nonfinancial ones.
- Calculating the cost savings due to fraud prevention is challenging but can provide a much more complete estimate of the total impact of fraud risk management.
- Leverage existing processes (e.g., internal control testing) and resources (e.g., data or staff) to secure management and staff buy-in, which can help prevent perverse incentives and gaming.
- Covert testing can safely identify weaknesses before fraudsters do and can provide unique insights into internal control vulnerabilities. It can also raise awareness among staff.
- Analyzing information on program responses to past fraud incidents can help managers determine what does and does not work.
- Programs should obtain and use feedback on the referrals they provide for investigation to determine how to improve both their internal controls and their referral processes.

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

In-Depth Example 3 of Evaluation Approach

Example 3: Perform a return on investment calculation

Return on investment provides one way of assessing fraud risk management efforts. ROI calculations compare benefits and costs of antifraud programs or investments to show how efficiently a project delivers results. These calculations can include both qualitative and quantitative factors. For additional guidance on comparing costs and benefits when assessing government programs, see OMB Circular A-94.[29]

The International Public Sector Fraud Forum provides guidance and examples of estimating the ROI in its *Fraud Control Testing Framework* guidance.[30] The formula includes calculating the amount at risk, the probability of risk, the current annual risk, the impact of the program or investment on the risk probability, the impact of the program or investment on the current annual risk, and the cost of the program or investment. With these values, managers can calculate the total costs and benefits over a given time frame to determine the ROI. See figure 5 below for an example.

Figure 5: Estimating the Financial Value of Preventing Ongoing Identity Compromise

Here is an example of how you might calculate the future loss prevented through ongoing identity compromise over a 5-year time horizon. To mitigate the threats to client identity information through phishing and social engineering, the department proposes to put service delivery staff through training twice per year and implement regular fraud control testing at a cost of $50,000 per year.

Formula	Example calculations
Amount at risk Calculate or estimate the amount at risk	Business impact: $1,500 per victim to remediate identities (notify, issue new identifiers and implement ongoing safeguards) Victim impact: $1,076 per victim and 34 hours per victim to repair the damage
Probability of risk Estimate the probability for compromise to occur with current controls	The risk currently occurs once every 5 days (73 identity compromises in the previous year)
Current annual risk	Total annual business impact: $109,500 ($146,000 annual impact for victims and 2,482 hours of remediation, or $38,533 of productive time) Total annual victim impact: $184,533
Impact of investment Determine the impact of the investment	The probability of risk is reduced by 10% per year over 5 years
Impact value Calculate the impact of the investment on the current annual risk	Year 1 - $10,950 business impact savings and $18,453 victim impact savings Year 2 - $21,900 and $36,906 Year 3 - $32,850 and $55,359 Year 4 - $43,800 and $73,812 Year 5 - $54,750 and $92,265
Total cost over 5 years:	$250,000
Impact value over 5 years:	• $164,250 in estimated business impact savings • $276,795 in estimated victim impact savings
Return on investment ratio:	**1.77**

Source: International Public Sector Fraud Forum, *Fraud Control Testing Framework*, FCTF-01 (Sept. 2023). | GAO-26-107609

Example 4: Measure cost savings from fraud prevention

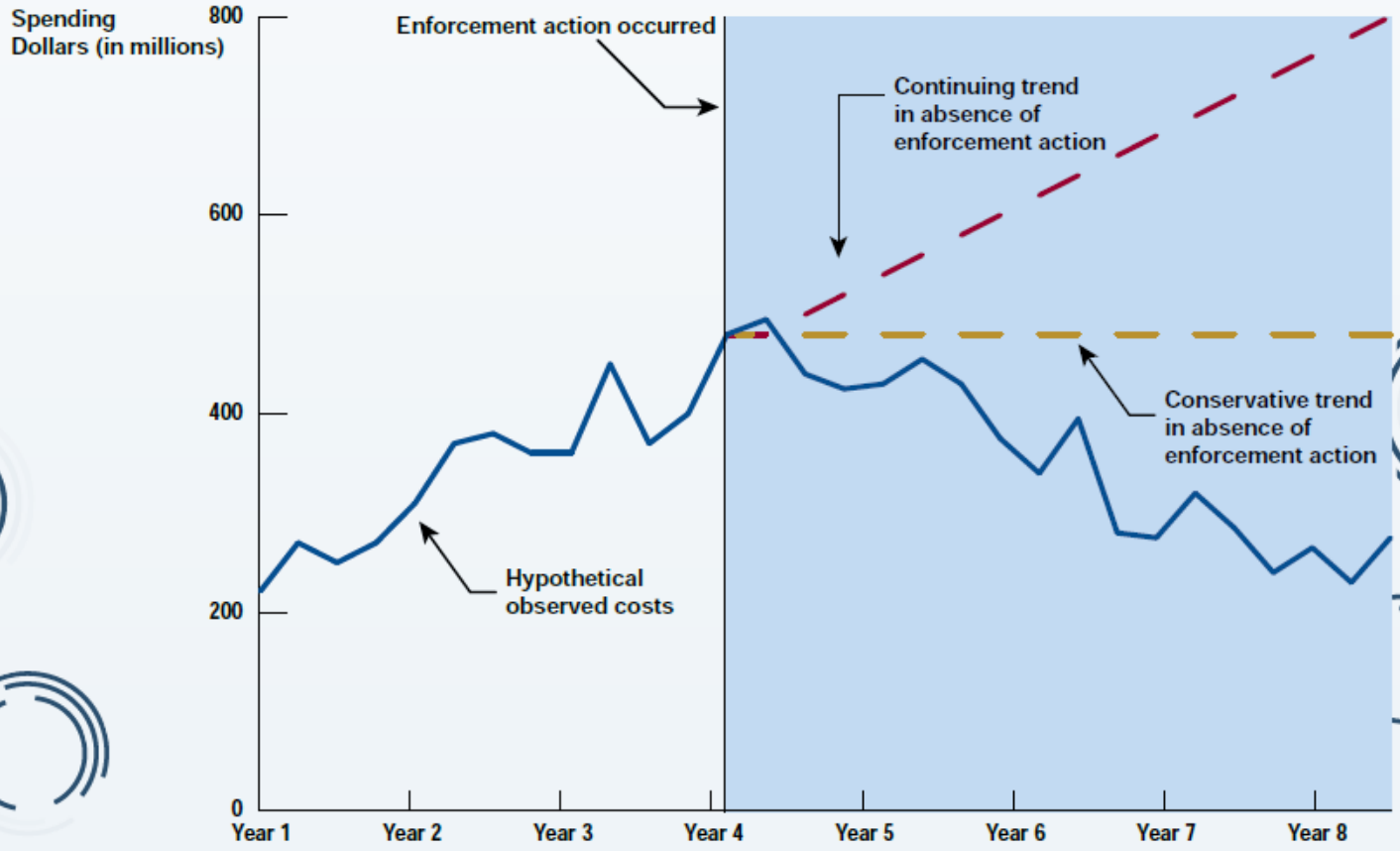
In 2024, the Healthcare Fraud Prevention Partnership (HFPP) published its white paper, *Measuring the Value of Healthcare Anti-Fraud Efforts*.[31] This paper focused on the importance of measuring and demonstrating the value of specific enforcement actions to prevent fraud, including through deterrence, since deterrence can provide greater financial savings than recoveries.

The HFPP provided steps to measure the impact of specific enforcement actions on deterrence:

1. Identify type of cost and enforcement action to monitor.
2. Determine time frame to measure costs before and after enforcement occurs.
3. Review data to determine and compare the preenforcement and postenforcement costs.
4. Use preenforcement costs to estimate the deterrence.

A steep spending decrease following an enforcement action can indicate that providers are deterred from conducting and billing for inappropriate procedures. Cost savings associated with deterrence can include both conservative and aggressive trend projections to provide estimated scenarios in the absence of the enforcement action, as depicted in a hypothetical example in figure 6.

Figure 6: Hypothetical Example of Cost Savings Information

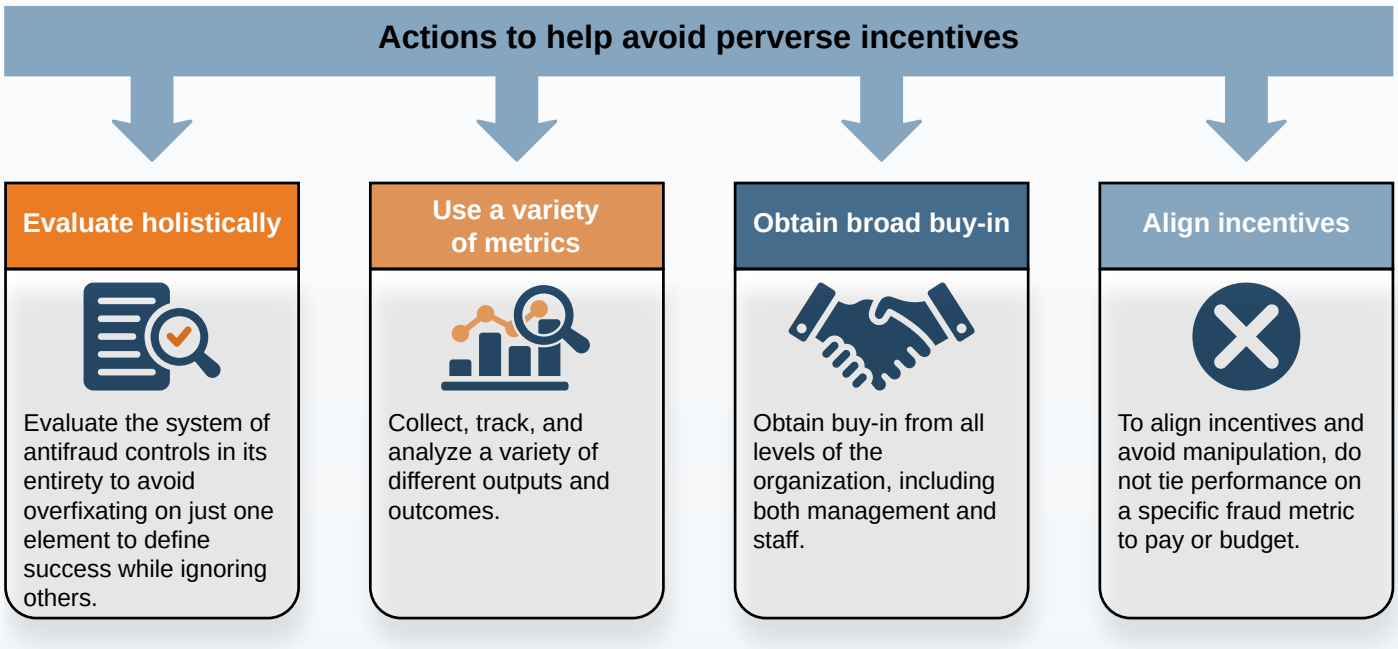


Source: GAO hypothetical example created from Healthcare Fraud Prevention Partnership information. | GAO-26-107609

Final Consideration...

The evaluations illustrated above are designed to strengthen the antifraud efforts of federal programs. Nevertheless, these kinds of evaluations can create perverse incentives to manipulate behavior if not carefully designed and implemented. For example, both programs and employees may seek to maximize their performance on a specific fraud-related measure at the expense of overall program integrity. A program's policies and procedures may prioritize investigations (response) instead of prevention to maximize the number of cases closed or number of convictions obtained. Fraud indicators can also be open to manipulation by employees, especially when linked to a reward, such as budget or pay. See figure 7 for examples of actions to help avoid perverse incentives.

Figure 7: Final Consideration: Avoid Perverse Incentives



Sources: GAO analysis of information provided by antifraud experts (info); Icons-studio/stock.adobe.com (icons). | GAO-26-107609

Endnotes

[1]Fraud involves obtaining something of value through willful misrepresentation. See GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 15, 2025), 8.06, 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]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). GAO also issued a web resource to help users learn more about fraud schemes that affect the federal government, such as their underlying concepts, and how to combat such fraud. GAO, "The GAO Antifraud Resource" (Washington, D.C.: Jan. 10, 2022), https://gaoinnovations.gov/antifraud_resource/. To better understand the potential extent of fraud, in 2024, GAO estimated total direct annual financial losses to the government from fraud to be between $233 billion and $521 billion, based on data from fiscal years 2018 through 2022. See GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments,* GAO-24-105833 (Washington, D.C.: Apr. 16, 2024).

[3]Pub. L. No. 115-435, 132 Stat. 5529 (2019).

[4]GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts*, GAO-23-105460 (Washington, D.C.: July 12, 2023). See also GAO-15-593SP and " The GAO Antifraud Resource." OMB has released specific guidance in various memorandums. For example, three memorandums—one each in 2019 (M-19-23), https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf, 2020 (M-20-12), https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-12.pdf, and 2021 (M-21-27), https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-27.pdf—provided detailed guidance on different aspects of Evidence Act implementation. See also Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, OMB Circular A-94 (Oct. 1992; revised Nov. 9, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/11/CircularA-94.pdf.

[5]U.S. Department of the Treasury*, Treasury Announces Enhanced Fraud Detection Processes, Including Machine Learning AI, Prevented and Recovered Over $4 Billion in Fiscal Year 2024* (Oct. 17, 2024), https://home.treasury.gov/news/press-releases/jy2650. Improper payments and fraud are two distinct concepts that are not interchangeable but related. Improper payments are payments that should not have been made or that were made in an incorrect amount, which can stem from various causes, including fraud. See GAO, *Improper Payments and Fraud: How They Are Related but Different*, GAO-24-106608 (Washington, D.C.: Dec. 7, 2023).

[6]In March 2020, Congress enacted the CARES Act, which created the Pandemic Response Accountability Committee within the Council of the Inspectors General on Integrity and Efficiency to promote transparency and conduct and support oversight of covered funds and the coronavirus response. In March 2021, the American Rescue Plan Act of 2021 appropriated $40 million to the Pandemic Response Accountability Committee, which subsequently established the Pandemic Analytics Center of Excellence. The role of the Pandemic Analytics Center of Excellence is to help oversee the trillions of dollars in federal pandemic-related emergency spending using advanced data analytics.

[7]GAO, *Small Business Administration: Progress and Work Remaining to Implement Key Management Improvement*s, GAO-24-107395 (Washington, D.C.: Mar. 6, 2024).

[8]International Public Sector Fraud Forum, *Fraud Prevention Savings Framework* (forthcoming).

[9]GAO, *National Institute of Standards and Technology: Strengthening Disclosure Requirements and Assessing Training Could Improve Research Security,* GAO-24-106074 (Washington, D.C.: Dec. 14, 2023).

[10]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.

[11]GAO, *Fraud Risk Management: Agencies Should Continue Efforts to Implement Leading Practices*, GAO-24-106565 (Washington, D.C.: Nov. 1, 2023).

[12]The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. The act further required OMB to incorporate the leading practices from GAO's Fraud Risk Framework in these guidelines. Pub. L. No. 114-186, 130 Stat. 546 (2016). The Fraud Reduction and Data Analytics Act of 2015 was replaced in March 2020 by the Payment Integrity Information Act of 2019, which required these guidelines to remain in effect, subject to modification by OMB, as necessary, and in consultation with GAO. Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131-132 (2020), codified at 31 U.S.C. § 3357.

[13]See OMB Memorandums M-19-23, https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf, M-20-12, https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-12.pdf, and M-21-27, https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-27.pdf.

[14]GAO, *Export-Import Bank: The Bank Needs to Continue to Improve Fraud Risk Management*, GAO-18-492 (Washington, D.C.: July 19, 2018).

[15]The Institute of Internal Auditors, Tone at the Top, *Auditing Culture*, Issue 124 (Lake Mary, FL: Aug. 2024), https://www.theiia.org/globalassets/site/resources/research-and-reports/tone-at-the-top/2024/august-2024-tone-at-the-top.pdf.

[16]United Kingdom Public Sector Fraud Authority, *Introduction to AI Guide with a focus on Counter Fraud* (Mar. 18, 2024), https://www.gov.uk/government/publications/introduction-to-ai-with-a-focus-on-counter-fraud/introduction-to-ai-guide-with-a-focus-on-counter-fraud-html.

[17]International Public Sector Fraud Forum, *Fraud Control Testing Framework*, FCTF-01 (Feb. 28, 2025), https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/fraud-control-testing-framework-fctf-01-html.

[18]Treasury Inspector General for Tax Administration, *Successful Detection and Assistance Processes Used to Combat Individual Identity Theft Should Be Implemented for Business Identity Theft*, 2022-40-041 (Washington, D.C.: July 27, 2022), https://www.oversight.gov/sites/default/files/documents/reports/2022-08/202240041fr.pdf.

[19]Internal Revenue Service, *Return on Investment: Re-Examining Revenue Estimates for IRS Funding*, 5901 (Feb.2024), https://www.irs.gov/pub/irs-pdf/p5901.pdf.

[20]Office of Inspector General, Pension Benefit Guaranty Corporation, *Detecting Fraud and Improper Payments Involving Deceased Participants,* (Washington, D.C.: Mar. 9, 2018), https://oig.pbgc.gov/pdfs/SR-3-9-18.pdf.

[21]Healthcare Fraud Prevention Partnership, *Measuring the Value of Healthcare Anti-Fraud Efforts* (Boston University: May 2024), https://www.cms.gov/files/document/measuring-value-healthcare-anti-fraud-efforts.pdf. The Healthcare Fraud Prevention Partnership is a voluntary public-private partnership that helps detect and prevent healthcare fraud through data and information sharing. Partners include federal and state agencies, law enforcement, private health insurance plans, and associations.

[22]Healthcare Fraud Prevention Partnership, *Measuring the Value*.

[23]U.S. Department of Health and Human Services, Office of Inspector General, *The Centers for Medicare & Medicaid Services Could Improve Performance Measures Associated With the Fraud Prevention System,* A-01-15-00509 (Washington, D.C.: Sept. 2017), https://oig.hhs.gov/reports/all/2017/the-centers-for-medicare-medicaid-services-could-improve-performance-measures-associated-with-the-fraud-prevention-system/; and information provided to us by officials at the U.S. Department of Health and Human Services, Office of Inspector General.

[24]International Public Sector Fraud Forum, *Fraud Control Testing Framework*, FCTF-01, https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/fraud-control-testing-framework-fctf-01-html.

[25]U.S. Department of the Treasury, *Estimating specific deterrence revenue from additional audits of high-income and high-wealth individuals* (Feb. 2024), https://home.treasury.gov/system/files/136/Specific-Deterrence-Paper.pdf.

[26]International Public Sector Fraud Forum, *Fraud Loss Measurement Framework* (Feb. 2025), https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/fraud-loss-measurement-framework-html.

[27]U.S. Department of Health and Human Services, Office of Inspector General, *UPICs Hold Promise To Enhance Program Integrity Across Medicare and Medicaid, But Challenges Remain,* OEI-03-20-00330 (Washington, D.C.: Sept. 2022), https://oig.hhs.gov/reports/all/2022/upics-hold-promise-to-enhance-program-integrity-across-medicare-and-medicaid-but-challenges-remain/.

[28]U.S. Department of Health and Human Services, Office of Inspector General, "OIG Modernization Initiative To Improve Its Publicly Available Resources – Request for Information," *Federal Register* 86, no. 2021-20558 (Sept. 24, 2021): 53072, https://www.govinfo.gov/content/pkg/FR-2021-09-24/pdf/2021-20558.pdf.

[29]See OMB Circular A-94, https://www.whitehouse.gov/wp-content/uploads/2023/11/CircularA-94.pdf.

[30]International Public Sector Fraud Forum, *Fraud Control Testing Framework.*

[31]Healthcare Fraud Prevention Partnership, *Measuring the Value.*

GAO Contact and Staff Acknowledgments

GAO Contact:
Rebecca Shea, SheaR@gao.gov

Staff Acknowledgments:
In addition to the contact named above, Heather Dunahoo (Assistant Director), Nicholas Weeks (Analyst in Charge), Colin Fallon, Lisa Fisher, Brooke Linsenbardt, Alanna Miller, Joseph Rini, and Samantha Sloate made key contributions to this report.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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, https://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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us

U.S. GOVERNMENT ACCOUNTABILITY OFFICE