Deloitte.

Federal CFO Insights

Real solutions to win the fight against improper payments and fraud, waste and abuse

Background

Federal agencies continue to make great strides to reduce improper payments and to mitigate the risk of fraud, waste, and abuse. Despite these efforts, the improper payments consistently remain a government-wide issue due to many reasons, such as the complexity of the payments and the balancing act that federal agencies need to perform to make timely payments while verifying all information are accurate before payment. The improper payment dollar estimate, attributable to 124 programs across 22 agencies in fiscal year (FY) 2014, was $124.7 billion, up from $105.8 billion in FY 2013.[1]

More than a decade has passed, since federal agencies had to comply with the Improper Payments Information Act of 2002 (IPIA), the first improper payment legislation. The next significant legislation related to improper payments followed the issuance of the American Recovery and Reinvestment Act of 2009 (ARRA). Due to the increased funding under ARRA, Congress passed more stringent improper payments requirements to mitigate the risk of improper payments with the Improper Payments Elimination and Recovery Act of 2010 (IPERA) and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA).

[1] https://paymentaccuracy.gov/

To help federal agencies achieve the goal of reducing improper payments, Congress has also passed progressive federal spending data legislations with the objective to bring accountability and transparency to federal agencies' management and US citizens. Learning from the passage of the Federal Funding Accountability and Transparency Act of 2006 (FFATA) and usage of the USA Spending.gov and the Recovery.gov websites, Congress passed the bipartisan Digital Accountability and Transparency Act of 2014 (DATA Act). The DATA Act's goal is to follow spending from congressional appropriation (how much, and for what programs, projects and activities) to the commitment and obligation (what goods and services, for what reason, and for whom) to disbursement of funds (amount, payment data and recipient), linked to receipts and financing (revenue and borrowing).

With these increased legislative requirements and enhanced data transparency, federal agencies' CFOs will have more resources to monitor and review funding under its improper payments programs. Due to the extensive changes in the data reporting structure and lack of guidance, the DATA Act will be gradually implemented at federal agencies. According to US Government Accountability Office (GAO), which conducted the audit between May 2015 and January 2016, a senior Department of Health and Human Services official told US Office of Management and Budget (OMB) and Treasury that without guidance about the "policy, process and technology changes that accompany the data element definitions," agencies can't effectively make implementation plans.[ii] Therefore, it is important for CFOs to consider what should be done now to address improper payments, fraud, waste and abuse while preparing for DATA Act compliance.

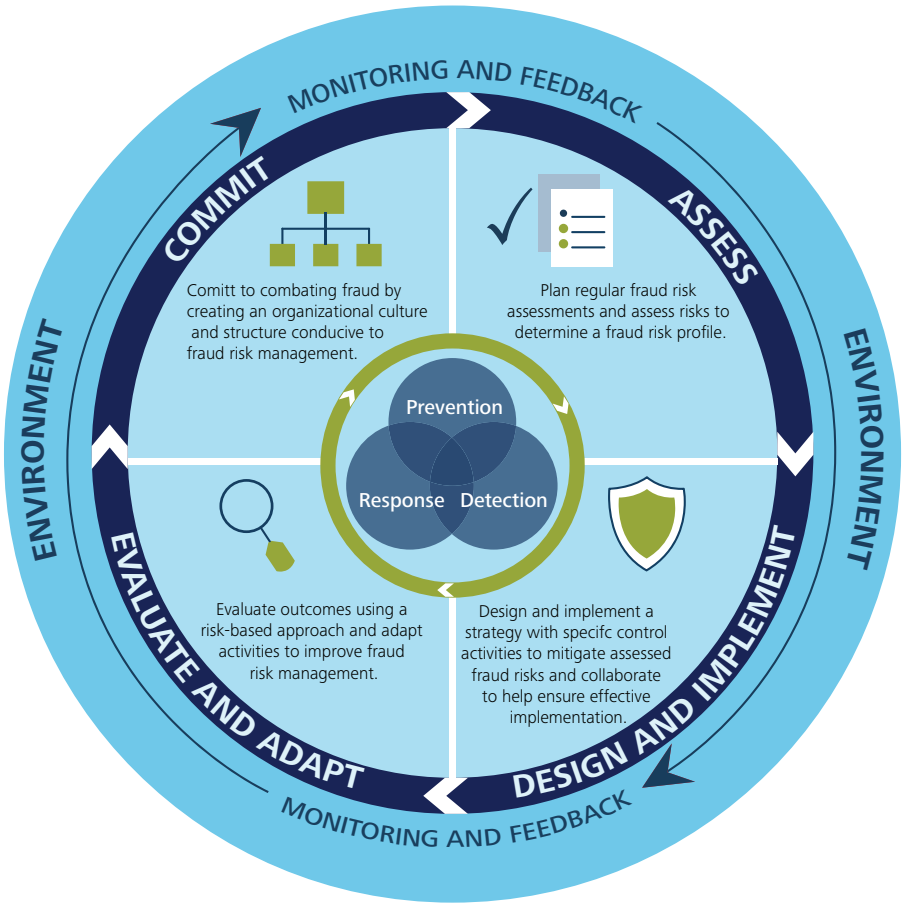
What can agencies do now to prevent improper payments

Recently, the GAO presented to the Congressional Oversight Committee on the progress that CFO federal agencies have made in combating improper payments and fraud, waste and abuse.[iii] This report provides a wealth of information on the trend of improper payments and highlights significant areas. For example, the report provided noncompliance with criteria in IPERA, strategies for using preventive and detective controls, potentially unreliable or understated estimates, programs that do not report on improper payments, improper payments resulting from fraud and root causes of the improper payments. Based on our review of the report and our assessment of the improper payments' results across agencies, we believe the following three actions can help strengthen federal agencies' strategies to mitigate the risks of improper payments:

1. Fraud risks assessment techniques for managing risks in a holistic framework
2. Continuous monitoring using data analytics with current data systems and using the Do Not Pay portal
3. Root cause analysis techniques to identify and implement effective Corrective Action Plans

The subsequent paragraphs will cover each of these three areas of improvement.

Implementing a framework for managing fraud risks in federal programs



Source GAO | GAO–15–503SP

[ii] NextGov "Watchdog: Agencies Need More Guidance Before They can Implement Data Act" by y Mohana Ravindranath, dated January 29, 2016

[iii] United States Government Accountability Office Fiscal Outlook Report "Addressing Improper Payments and the Tax Gap Would Improve the Government's Fiscal Position", dated October 1,2015

Agencies will benefit from taking an all-inclusive approach to fraud detection, leveraging an enterprise view of the people, processes, technology, data, and analytic techniques necessary to adopt a proactive stance against fraud, waste, and abuse. CFOs should commit to a framework that continuously mitigates the risk and likelihood of fraud by monitoring and adapting to the environment. The GAO performed a study of the risks threatening federal programs and established the GAO Fraud Risk Management Framework,[iv] which incorporates a set of leading practices for CFOs to identify and mitigate fraud risks.

The GAO framework provides an agency's leadership with guidance on how to effectively employ risk management activities through four steps — (1) Commitment, (2) Assessment, (3) Design and Implementation, and (4) Evaluation and Adaption. As the risk environment evolves, fraud risks should be continuously monitored, and feedback should influence the controls and framework in place.

Commit — Leadership is key in demonstrating integrity and setting the tone to create a fraud detection culture rooted in the organization. A commitment should be made by senior leadership to the prevention, detection and response to fraud, creating a culture dedicated to managing and combatting risks facing the agency from the top-down.

CFOs must be vigilant in maintaining this commitment to an antifraud culture; it is not enough to rely solely on an initial commitment to develop the framework, but a constant presence of CFOs' commitment is integral to the continued success of the programs. Engaging each individual at all levels of an agency reinforces the culture throughout and increases the likelihood that fraud can be prevented.

Assess — CFOs should consult with internal and external stakeholders, such as general counsel or contractors, who may be able to provide additional insight into potential fraud risks threatening the program. No two programs will be alike in the inherent risks threatening an agency; therefore, each risk assessment must be tailored based on the program. To fully assess and understand the fraud risks, the following actions should be considered:

- Identify inherent fraud risks affecting the program
- Assess likelihood and impact of inherent fraud risks
- Determine risk tolerance
- Examine the suitability of existing fraud controls and prioritize residual fraud risk
- Document the program's fraud risk control[v]

Design and Implement — After fraud risks are identified, a strategy should be designed to mitigate these risks with the focus again placed on the prevention of the assessed risk. A fraud response plan should also be developed which may include accepting, reducing, sharing or avoiding the risk. Control activities should be evaluated, and costs and benefits should be reviewed to determine a balance between successfully executing the goals of the agency and effectively managing this risk. CFOs should work to identify the amount of risk they are willing to accept when evaluating the controls to be implemented. Effective implementation relies on the involvement and collaboration of those involved at all levels.

Evaluate and Adapt — The creation and implementation of a strategy relying on control activities designed to combat fraud risks, and the commitment to understand, monitor, analyze and adapt to the ever-changing threat environment, both internally and externally, when deployed strategically, may allow an agency to take steps to mitigate the likelihood of fraud occurring. CFOs must understand, however, that risk cannot be completely eliminated, and controls must be evaluated to achieve an equilibrium of effective use of resources to prevent, deter and respond to fraud while achieving the goals and missions of an agency.

[iv] United States Government Accountability Office "A Framework for Managing Fraud Risks in Federal Programs", dated July 2015

[v] United States Government Accountability "A Framework for Managing Fraud Risks in Federal Programs", dated July 2015, page 6

Employing continuous monitoring using data analytics with current data systems and using the Do Not Pay portal

Agencies will benefit from implementing an integrated continuous monitoring platform containing a cross-section of capabilities to provide an effective vehicle for improper payment mitigation both now and into the future.

Strategic deployment of data analytics can be used in many powerful ways, including identifying improper payments, providing operational insight into the agency as a whole as well as the decentralized field offices, and assist in identifying risks that may not currently be on the radar. Data analysis is the key to helping agencies become risk intelligent in managing the decision-making process for both up and downstream. Data-driven decision making and corresponding preventative measures can be leveraged in the face of meeting and exceeding government guidance, political pressures, Office of Inspector General (OIG) audits and public scrutiny. Indeed, the DATA Act gives further credence to the weight our nation's federal leadership is placing on the power of data analytics to help bring even more transparency and operational intelligence to the government.

This platform can include real-time detection, data matching, and predictive analytics.

- **Real-Time Detection** — In the case of improper payments, an effective strategy involves deploying a technical infrastructure designed to prevent disbursement of these funds. Continuous monitoring technology provides the capability to analyze payment data in near-real time and queue up potential problems for review before disbursement. By doing so, organizations can move from "pay and chase" to "protect and prevent" and provide the technological capability to accelerate follow-up reviews.
- **Data Matching** — In addition to the wealth of data available internally to empower an agency's decision ability, a tremendous amount of data also exists externally. When federal agencies scope out their problem sets, it will be critical that they consider what external data sets might be available to help mitigate these issues. For example, OMB has been tasked with developing a Do Not Pay portal to assist agencies to reduce improper payments.

  The Do Not Pay portal is a tool that helps prevent improper payments before a contract is signed or before funding the disbursement. The portal enables agencies to verify payments against the other federal data sources to flag a potential improper payments and/or debarred vendors for further research.

  If an agency can cross-reference its transactions or procurements against this type of database in real-time, CFOs will have inherently reduced its propensity for making improper payments.
- **Predictive Analytics** — Economists, statisticians, and decision scientists have long used predictive analytics to uncover patterns and outliers buried in a variety of databases. Predictive analytics involves judiciously applying advanced data mining techniques to identify patterns and outliers and to make predictions about future events. A thorough understanding of data can provide insights into which disbursements are indicative of improper payments.
- An organization that understands the exciting potential of these capabilities—and begins visioning the "what" and "where" it can be deployed—will have a powerful new tool to protect assets and optimize operations. Preventing an improper payment from occurring is vital strategy to combat improper payments rather than trying to collect an erroneous payment. By implementing effective continuous monitoring and using the tools available (i.e., Do Not Pay portal), CFOs can greatly enhance the likelihood of that resources are properly deployed to the efforts supporting their programs' missions.

Implementing the root cause analysis techniques and effective Corrective Action Plans

Agencies will benefit from conducting a thorough root cause analysis of their improper payments. The root cause analysis should be performed to understand the reason behind the improper payment (e.g., if all issues occurred in a particular period of time there may be a discrete, identifiable cause). Next, a determination should be made as to whether the conditions which led to the improper payment still exist, such that they might occur again in the future.

Corrective Action Plans should be developed to address specific root cause of the improper payment occurrence, and include the following elements:

- **Develop a Realistic Timeline** — Milestones should be developed and be specific, realistic, and obtainable.

- **Develop Test Plan and Perform Testing** — Test plans should be developed to verify that the corrective actions effectively mitigate the risk of future improper payments. These corrective actions can include IT system upgrades, policies changes, improvements in internal controls, and/or other human capital related training and employee oversight changes to address the root cause of why the improper payment occurred.
- **Key Performance Measures** — The performance measures should be objective, measurable, and quantifiable. Performance measures can assist the project managers with determining if any changes in strategy are required to meet targeted milestones under the Corrective Action Plan.

Year after year, the same reasons for improper payments have been identified without an effective solution to mitigate the risk of future improper payments. CFOs can benefit from working with their program leadership to truly identify the reasons for the improper payments and work to put into place solid corrective action plans to resolve the issues and mitigate the risks going forward.

Benefits to CFOs of reducing improper payments

Taxpayer focus on government spending is at an all-time high, and the CFO is the agency's best champion for making certain funds are used for their intended purpose through implementing a holistic improper payment program. By implementing an all-inclusive approach to assess improper payments using prevention and detection techniques, including fraud risk assessment analysis, data analytics, continuous monitoring and corrective action root cause analysis, CFOs have a unique opportunity to collaborate with program managers and support their agencies in optimizing the use of funds to achieve agency mission objectives and contribute to citizen-centric reports/services and government-wide long term plans.

Contact Us

Haideh Chubin
Director
Deloitte Advisory Deloitte & Touche LLP
hchubin@deloitte.com

Jaclynn Campbell
Specialist Leader
Deloitte Advisory Deloitte & Touche LLP
jaccampbell@deloitte.com

Deloitte Federal CFO Insights are developed with the guidance of Roger Hill, Principal, Federal CFO Program Leader, Deloitte & Touche LLP; and Emily Franklin, Matt Prizinsky, and Natalie Samuel, Federal CFO Program Managers,

Deloitte Consulting LLP
For more information about Deloitte's Federal CFO Program, visit our website at: Deloitte Federal CFO