KPMG

Strengthening integrity in government programs

Strategies to elevate payment integrity and defend against fraud in the federal government

Current federal environment

The US federal environment continues to confront long-standing issues that compromise payment integrity, including fraud, waste, abuse, improper payments, and outdated technology. For example, the US government faces substantial vulnerabilities and inefficiencies in various areas, including healthcare fraud, siloed operations, and unintegrated information technology (IT) systems. Delayed adoption of advanced security models further exacerbates these problems, resulting in significant economic losses and threats to a program's mission success. Fraud and misuse of government resources divert these resources from their intended purpose, which undermines public trust and leads to inefficiencies that hinder economic progress with estimated losses ranging from $233 billion to $521 billion annually due to fraud alone.[1]

Against this backdrop, there is a resolute determination to address these systemic issues. Principal goals include reducing costs, improving accountability, increasing financial integrity, centralizing systems, streamlining reporting, developing specific transparency measures, updating technology, and optimizing operational outcomes. This comprehensive approach, if executed thoughtfully through targeted initiatives led by collaborators like KPMG LLP (KPMG), can put government agencies on the path to make substantial progress in helping to ensure that taxpayer funds are utilized effectively and public trust in government operations is fortified.

Addressing fraud, improper payments, cyber threats, and technology opportunities

Bad actors are maximizing use of advanced cyber threats and malicious actions capable of causing catastrophic damage in today's digital world. A prime example is the increase in ransomware attacks, such as the February 2024 attack on UnitedHealth's subsidiary Change Healthcare that resulted in UnitedHealth paying a $22 million ransom and reporting total losses of as much as $872 million. The attack by the Russia-based cyber group BlackCat shut down operations at hospitals and pharmacies across the country for more than a week. More alarmingly, it resulted in the theft of more than six terabytes of data, including personal data and sensitive medical records.

In the face of such threats and complexities, addressing fraud, waste, abuse, improper payments, and outdated technology is critical—especially for many stakeholders, such as program beneficiaries, government agencies, C-suite executives, program managers, and taxpayers. Implementing risk-based assessments can enable faster, more informed decision-making, provide detailed operational insights, cost savings, more accurate operations, mission focus, and greater accountability—all effective tactics to combat known threats. For government agencies, adopting these measures enhances resource allocation efficiency, improves service delivery, and reinforces public trust by mitigating risks such as data breaches and the influence of bad actors. Meanwhile, program beneficiaries will continue to receive hard-earned benefits while taxpayers can rest assured knowing their contributions are safeguarded, reducing unnecessary taxation and enhancing service reliability.

The critical need for risk mitigation in the context of fraud, waste, and abuse cannot be overstated. The landscape of cyber threats is continually evolving, and government entities are increasingly vulnerable to advanced persistent threats and cyber-attacks. Efforts to address these risks should include specific integration of innovative technologies. The use of specialized tools and advanced analytics, as evidenced by 48 percent of organizations with centralized risk resilience structures, highlights the potential for better risk prediction and management (KPMG Enterprise Risk & Resiliency Survey). However, technology alone is insufficient—effective program administration anchored in clear policy frameworks is essential. This approach aligns with findings from our KPMG Enterprise Risk and Resiliency Survey, where precise governance structures have proven to enhance efficiency, capability, and maturity in handling disruptions. By incorporating innovative technology, advanced data analytics, and a strong risk-based governance framework, organizations can effectively manage and mitigate risks, improve resilience, and ensure optimization of both resources and operations.

[1] US Government Accountability Office. "Fraud and improper payments," March 2025. Retrieved July 11, 2025, from https://www.gao.gov/fraud-improper-payments.
[2] KPMG LLP. "KPMG Enterprise Risk & Resiliency Survey," March 2025. Retrieved July 11, 2025, from https://kpmg.com/us/en/media/news/kpmg-risk-resilience-survey-2025.html.

The intersection of fraud, improper payments, cyber threats, and technology

When thinking about the relationship between fraud, improper payments, cyber threats, and technology, it is easiest visualized as intersecting and overlapping components. Fraud, waste, and abuse collectively contribute to the larger issue of improper payments. For instance, improper payments can result from fraud (e.g., intentional falsified claims), waste (e.g., duplicate payments from process errors), or abusive behaviors (e.g., payments for services not received). These components can facilitate each other—lax verification may enable fraud and outdated systems can create vulnerabilities to exploitation.

Surrounding these components, cyber threats act as external force multipliers, striking at the vulnerabilities within the system. For example, a breached database can result in identity theft and fraudulent claims, while a ransomware attack can cause payment errors by disrupting controls. Therefore, modern fraud schemes often incorporate a cyber element, necessitating robust cybersecurity efforts intertwined with fraud prevention.

Crucially, technology can act both as a tool and a threat. While advanced technology like artificial intelligence (AI), analytics, and automation can enhance fraud detection, reduce improper payments, and improve controls, bad actors can also exploit it. This duality underscores the importance of harnessing technology for defense while mitigating its malicious use. Sustained program improvement must keep pace with evolving threats to maintain program integrity.

Tackling fraud with practical solutions

Fraud in the government context diverts critical resources, undermines program integrity, jeopardizes our most vulnerable citizens, and erodes public trust. While many government programs are plagued by the use of legacy systems or the mismanagement in implementation of a modernized IT system, government leaders must also be aware of the potential fraud vulnerabilities ripe for exploitation due to architectural obsolescence, data silos, and limited integration capabilities.

Here are some practical solutions for identifying and preventing fraud, while optimizing technology:

1 Implement a Fraud Risk Management (FRM) initiative

Establish a comprehensive approach that includes regular risk assessments, robust internal controls, and clear response plans. A robust FRM program involves leadership and staff commitment to an antifraud culture, fraud risk assessments, control assessments, antifraud training, strategy, collaboration with internal and external stakeholders, metrics to measure the effectiveness of those activities, and fraud awareness activities.

2 Conduct fraud risk assessments

Evaluate fraud exposures in areas like procurement, payroll, and benefits payouts and ensure management commits to mitigating these risks. After evaluating fraud exposure, conduct risk assessments to identify the likelihood and impact of the risk to the program and prepare a fraud risk profile. Then, identify mitigation strategies and responses to lessen the risk of fraud, waste, and abuse. A fraud risk exposure analysis can assist with prioritizing risk assessments to those at a higher risk.

3 Use Business Activity Monitoring (BAM)

Implement real-time BAM systems to detect and respond to fraudulent payment transactions as they occur. BAM tools track and analyze live transaction data across various business processes, providing immediate alerts for potentially suspicious activities. This proactive approach ensures quicker intervention and minimizes potential damage.

4 Leverage AI for prevention

Utilize machine learning to analyze vast data sets in real time, detect anomalies, and predict potentially fraudulent behaviors. AI-enabled intelligent systems adapt to recognize and guard against emerging threats, continuously adjust to changes in use patterns over time, and provide high-level reasoning to reduce false alarms and predict and/or flag future data anomalies that may indicate the presence of fraud.

5 Establish incident response processes

Have forensic accounting and investigation teams ready for prompt detection and rigorous investigation. Leveraging the right personnel to thoroughly investigate instances of fraud is crucial as these experts possess specialized skills in analyzing complex financial data and uncovering deceptive practices, which supports agency legal actions to recover lost resources and deter future fraud.

6 Use case management tools

Utilize case management tools to enhance the efficiency and effectiveness of investigative processes by centralizing information and tracking activities in real time. Effective case management tools, especially when enabled by AI, streamline and increase productivity within a workflow, allow for better coordination among departments, and help ensure instances are thoroughly investigated and addressed. Furthermore, case management systems provide valuable data analytics capabilities, helping to identify patterns and trends that may indicate fraudulent activities, thereby enabling proactive measures to prevent further occurrences.

7 Data analytics dashboards

Interactive dashboards help visualize fraud risk indicators, making complex data accessible and aiding decision-making. Real-time updates to dashboards provide a real-time view of the overall system state and operating environment, enabling rapid recognition and response to threats.

By integrating these solutions, government programs can achieve their mission while protecting themselves against fraud, thereby safeguarding resources, maintaining program integrity, and ensuring public trust.

Minimizing waste efficiently

Internal inefficiencies (i.e., waste) drain resources and hamper effectiveness. Addressing this demands specific technological updates and strategic planning.

We have identified a few key considerations that can help place government programs on the path to eliminating waste and increasing efficiency:

1 » Apply AI for efficiency

Automate processes and employ predictive analytics to enhance productivity, reduce duplicate efforts, and focus resources on critical areas. Automating routine but time-consuming tasks, such as processing forms and documents, provides substantial gains in efficiency. Government workflows, such as financial operations, follow complex sets of standard operating procedures (SOPs)—by applying AI and predictive analytics solutions to these SOPs, organizations can recognize actions that will cause exceptions or errors later in the workflow and pre-emptively fix errors or reject the case, reducing waste of processing time and resources.

2 » Design compliance programs

Refine and consider centralizing compliance programs to focus on the most value-added activities, helping to address the most pressing and highest risk within a program, while removing potential redundancies. To further refine, agencies should leverage advanced technology tools such as AI and machine learning to automate monitoring and reporting processes within the compliance program. Incorporate data analytics to perform comprehensive risk assessments, identifying areas of inefficiency and waste, and to help drive the intensity of the compliance procedures. Through continuous analysis of real-time data, organizations can quickly address compliance issues and optimize resource allocation, while ensuring waste reduction and maximizing efficiency.

3 » Update legacy systems

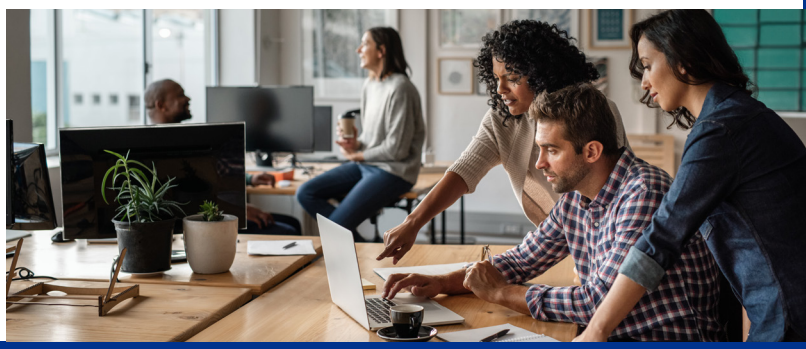
Integrate systems to improve data quality through effective data management and operational enhancements. Many government systems are highly stove-piped or separated from one another, each with their own data systems. The result is often duplicated data and processes, along with the introduction of data integrity concerns when systems do not agree. Effective modernization with a focus on stakeholder needs, coupled with robust change management, will help agencies reduce system vulnerabilities while increasing productivity in operations, reporting, and decision-making.

4 » Implement payment controls

Use prepayment validation to verify the accuracy and eligibility of transitions before any funds are disbursed—thus eliminating the need to pay and chase, whereby unauthorized payments are stopped prior to disbursement. Complement this with thorough postpayment audits to review and confirm the validity of payments made to identify and address discrepancies. This dual approach ensures a robust system that minimizes improper payments and maintains financial integrity.

5 » Set accountability metrics

Deploy real-time dashboards to monitor financial, operational, and quality indicators continuously. These dashboards enable quick identification and response to deviations, ensuring that any issues are promptly addressed.



Preventing and addressing abuse

Abuse involves the misuse of authority or resources, primarily internal. Addressing abuse is crucial for safeguarding public resources, maintaining performance standards, and ensuring the effectiveness of federal programs. Technological advancements can help mitigate abuse but also pose new vulnerabilities that need strategic countermeasures.

To help reduce instances of abuse and show the value of government programs, consider these initial steps:

1 Establish clear policies

Implement unambiguous regulations, policies, and processes; document them thoroughly; and ensure resources receive adequate training. Work with program managers to perform a frequent review of the applicability of established policies, and incorporate any lessons learned and/or improvement of processes based on other review activities or the implementation of technology.

2 Supervised oversight

Alternate responsibilities to prevent unchecked control and employ AI assistance for task management enhancements.

3 Behavioral data analysis

Use analytics to detect subtle anomalies or patterns indicative of abuse. Implementing knowledge graphs and graph analytics provides insight into higher order relationships such as coordinated efforts of groups of bad actors that would otherwise go unnoticed. Implementing a regular cadence of behavioral data analysis helps to prevent systemic issues from developing over time.

4 Conduct comprehensive audits

Conduct comprehensive audits by regularly implementing technology-assisted audits and assessments to identify potential abuses. Leverage advanced technology for thorough examination and real-time analysis to identify, detect, and address irregularities or vulnerabilities quickly.

5 Secure AI use

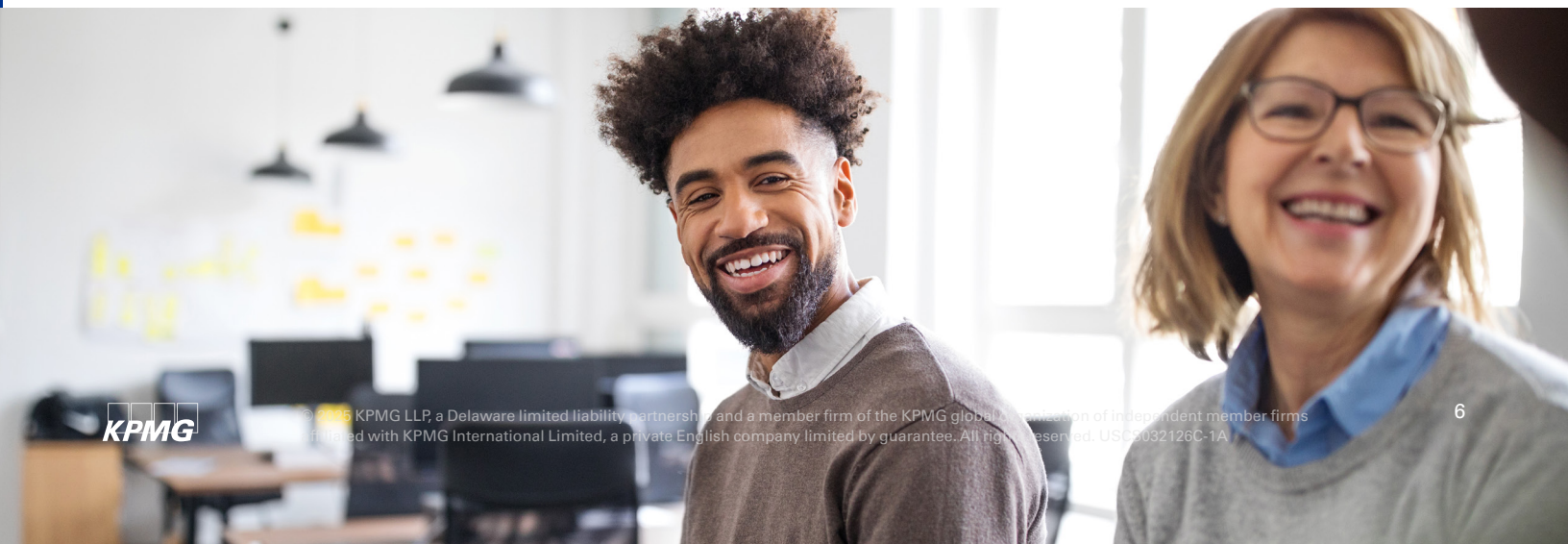
Ensure transparent governance and robust cybersecurity frameworks to prevent the exploitation of AI. This is especially important as bad actors increasingly leverage AI to improve their attack methods and to serve as an attack point. A lack of proper governance and AI policy increases the risk of internal misuse of AI systems and tools that can easily expose sensitive data to privacy attacks.

Conclusion

To safeguard against fraud, waste, abuse, improper payments, cyber threats, and outdated technology, C-level executives and program managers should prioritize activities that will result in thoughtful and positive changes that have a long-term impact on the program mission, government employees, and the American people. While the issues and threats are large and looming, incremental strides towards improvement and reframing issues as opportunities will help agencies take the first step in a stronger, more efficient, and accountable government. Leadership should prioritize specific objectives that focus on program mission, results, accountability, transparency, security, efficiency, and technology effectiveness. Through the following efforts, we can help agencies generate efficiencies, increase transparency, and modernize systems:

- **Defined fraud prevention and detection**—Establishing a defined FRM initiative and using AI strategically will help reduce fraudulent activities, helping ensure resources are directed to essential activities.
- **Increased operational efficiency**—Automating tasks and modernizing systems to streamline operations, cut errors, and expedite mission success allows employees to focus on tasks that require direct oversight.
- **Improved transparency and accountability**—Leveraging real-time data analytics and collaborative data sharing across agencies, combined with sophisticated analysis tools and centralized case management, enhances operational visibility and accountability. This thorough approach enables leaders to gain instant insights into program health, facilitating informed and timely decision-making.
- **Cost reduction**—Deploying prepayment checks and a thorough compliance strategy, including technology assisted audits, real-time quality assurance reviews, and investigations, can reduce errors and unnecessary expenditures, leading to significant cost savings.

The solutions noted throughout this paper are thoughtfully crafted and tailored to the specific needs of the agency and/or program and sprinkled with the ingenuity to implement these solutions in a practical manner (i.e., implementation facilitated by more output-focused contracting, more research and development, more data exploration, more process and technology pilots, more innovative compliance approaches and consequences, more centralization of capabilities, more automation and AI, etc.) to drive positive change and enhance the credibility of federal programs.



Contact us

Tim Comello
Partner, Federal Advisory
T: +1 202 430 0637
E: tcomello@kpmg.com

John Iannacone
Director, Federal Advisory
T: +1 267 256 3069
E: jgiannacone@kpmg.com

Safa Khaleq
Managing Director, Federal Advisory
T: +1 571 512 8032
E: skhaleq@kpmg.com

Ning Wang
Director, Federal Advisory
T: +1 214 840 2409
E: ningwang1@kpmg.com

Brittany Gaines
Director, Federal Advisory
T: +1 313-738-0229
E: bgaines@kpmg.com

Learn more

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**