Fighting fraud in Federal programs

Antifraud efforts utilizing fraud risk management activities and fraud data analytics to combat waste, fraud, abuse, and mismanagement within Federal programs

Fraud, waste, and abuse (FWA) pose significant threats to the integrity and effectiveness of Federal programs, siphoning off billions of dollars annually[1]. The Government Accountability Office (GAO) has extensively reported on this issue, showcasing a wide array of fraud schemes that exploit weaknesses in various program controls. Key examples of fraud schemes include contract and procurement fraud (e.g., bid-rigging, kickbacks)[2], grant fraud (e.g., false claims, embezzlement), and beneficiary fraud (e.g., identity theft, false eligibility). Given the complexity and sophistication of modern fraud tactics, Federal agencies need to adopt innovative, proactive measures to safeguard taxpayer funds and maintain public trust. It is now imperative to quickly eliminate unnecessary spending through a focused effort on procurement and contract management, leveraging spend analytics, technology modernization, organizational transformation, data and analytics, and risk management[3] to pave the path forward.

Federal agencies should leverage the GAO's Fraud Risk Management (FRM) Framework[4] by implementing a proactive, risk-based approach to combating fraud. The FRM Framework, along with legislation like the Fraud Reduction and Data Analytics Act[5], requires agencies to conduct fraud risk assessments, develop antifraud controls, and use data analytics to detect, prevent, and monitor fraud. These approaches not only enhance the capacity to detect and prevent fraud but also position agencies to respond effectively to emerging threats.

Key FRM activities that agencies should implement along with their benefits include:

Qualified electing fund (QEF)

Conducting fraud risk assessments and implementing mitigation controls are essential for organizations to prevent and detect fraudulent activities:

- Develop a fraud risk assessment plan/fraud risk exposure analysis
- Conduct data-driven fraud risk assessments to identify highest fraud risks and evaluate for likelihood and impact
- Analyze historical fraud cases and identify patterns and red flags
- Develop mitigation plans and antifraud controls to prevent and detect fraud
- Establish governance, roles, and responsibilities for managing fraud risk
- Establish policies, standard operating procedures, and strategy documentation
- Provide fraud awareness training to employees

Key benefits: Proactively identifies and mitigates top fraud risks before they occur, preventing financial losses and reputational damage.

Mark-to-market (MTM)

To be effective, agencies need to take an enterprise approach to fraud data analytics, integrating data across multiple internal and external sources. This provides a more comprehensive view to detect sophisticated fraud schemes that may occur across multiple programs or systems. Agencies also need to invest in data analytics tools and skill sets, either developing in-house capabilities or working with professional services firms like KPMG:

- Leverage advanced data analytics tools (e.g., machine learning, AI) to continuously monitor transactions for red flags in real time
- Develop risk scoring models and interactive dashboards to detect anomalies and prioritize high-risk cases for investigation

[1] Source: Government Accountability Office (GAO), "2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud" (2024)
[2] Source: Government Accountability Office (GAO), "Defense Procurement" (2019)
[3] Source: Procurement Sciences: "Understanding and Preparing for: Department of Government Efficiency (DOGE)" (2025)
[4] Source: Government Accountability Office (GAO), "A Framework for Managing Fraud Risks in Federal Programs" (2015)
[5] Source: Congress, "Fraud Reduction and Data Analytics Act of 2015" (2015)

Key FRM activities that agencies should implement along with their benefits include: (continued)

Third-party risk management

- Conduct due diligence on high-risk vendors and grantees, reviewing financial stability, ownership, and past performance issues
- Discover hidden relationships, cyber threats, insider threats, and risk from foreign ownership that may enable fraud
- Continuously monitor vendor transactions and performance to detect billing fraud, product substitution, and other schemes
- Identify vendor relationships posing fraud or reputational risk

Key benefits: Detect vendor fraud schemes like bid-rigging and kickbacks while preventing organizations from doing business with unethical third parties.

Mark-to-market (MTM)

After conducting fraud risk assessments and performing fraud data analytics, agencies often need to take further measure to investigate and remediate potential instances of FWA. Having the ability to quickly and efficiently deploy a team to conduct these investigations is integral to any agency successfully eliminating fraud, waste, and abuse from its programs:

- Develop and design a regulatory enforcement methodology and step-by-step investigation procedures
- Assist with reactive investigations into suspected waste, fraud, and abuse incidents
- Conduct ongoing compliance investigations and assist with enhancing controls to mitigate identified schemes.
  Key benefits: Provide skilled resources to support investigations, determine root causes to prevent repeat incidents, and recover funds.

Competing priorities, resource constraints, and lack of expertise pose challenges for Federal agencies when developing an antifraud program. As a result, fraudsters continue to find opportunities to steal Federal funds, often using increasingly sophisticated schemes that are difficult to detect. New and emerging fraud schemes, like synthetic identify theft, fraud-as-a-service, and deepfake technology pose an even greater threat. This puts agencies at risk of significant financial losses, as well as reputational damage that erodes public trust. Investing in FRM services can help agencies overcome these challenges and implement the critical activities needed to prevent, detect, and respond to fraud.

Effective FRM also requires close collaboration across different departments (e.g., program offices, information technology, finance) and with external partners (e.g., law enforcement, other agencies). Breaking down silos and fostering a culture of information sharing is critical to detecting and preventing fraud. Agencies should also be aware of potential challenges in ensuring data quality and integrating disparate data sources, and work to implement solutions (e.g., data governance, master data management) to overcome these hurdles.

Working with experienced firms like KPMG LLP can help accelerate this journey. KPMG brings deep experience in FRM, data analytics, and technology integration. We can help agencies design, implement, and operationalize a data-driven FRM program tailored to their unique needs and environment. By providing leading tools, methodologies, and talent, KPMG enables agencies to realize the benefits of advanced fraud detection and prevention faster and with less risk.

Implementation considerations

When implementing a FRM program, agencies should follow leading practices such as:

- Securing buy-in and support from senior leadership
- Starting with a pilot program focused on the highest risk areas
- Establishing clear metrics and key performance indicators to measure success
- Implementing continuous monitoring, testing, and refining antifraud controls to keep pace with evolving threats.

Fraud, waste, and abuse analytic framework

KPMG approaches the FWA problem set in a unique fashion by offering our client an end to end solution. Instead of solely focusing on a particular technique, algorithm, or technology for anomaly detection, our FWA Analytic Framework is structured in four pillars. Each pillar employs several interdisciplinary, data-driven techniques and is based on best practices from helping our client prototype and implement fraud detection programs.

Sense & deter

- **Understand what is normal:** rely on legacy data, benchmark, add process controls.
- **Focus on precision sensing:** model individual behavior, not cohorts.
- **Use behavioral economics:** influence the fraudsters, force them away from vulnerable channels, direct them to contained areas will less impact or drive away entirely.
- **Add feature richness:** utilize external richness: utilize external datasets (Econometric Data, US Census, resumes, Social Media, Facebook, LinkedIn).

Detect

- **Try multiple data models:** rely on simpler techniques, but also try advanced methods (Neural Networks, Support Vector Machines, Decision Trees, Random Forests, Regression, Ensemble Models).
- **Model management is key:** overlap your analysis, understand when to refactor and retire models.
- **Streaming detection:** monitor and detect real time fraud.
- **Robotic processes:** automate all manual data entry to all manual data entry to the extent possible.

Prevent

- **One size does not fit all:** understand risk segments and fraud profile, develop custom strategies for each.
- **Implement safeguards:** develop not just one safeguard but an array to catch residuals.
- **Triage transactions:** not all seemingly suspicious transactions are fraudulent-careful selection of non-traditional filters can help to reduce the pool.
- **Remember the tradeoffs:** between accuracy and precision. How many False Negatives are acceptable?

Recover & optimize

- **Prioritize and manage cases:** dynamically score cases, consider ROI and utility of case, provide feedback to detection models.
- **Investigate, pursue, and recover:** establish tractable collections ROI, use portfolio optimization. Collect outcome data for continuous improvement, feedback to learning models.
- **Use behavioral economics:** incorporate additional measures to enhance the culture of compliance at all levels to remove vulnerabilities that breed misconduct.

In summary, a robust FRM management program incorporating these key activities enables agencies to meet GAO and legislative requirements while proactively combating fraud and safeguarding taxpayer funds. Analytics and due diligence provide crucial monitoring to quickly detect issues, while governance and training promote an antifraud culture. Collaboration and continuous improvement are also essential for staying ahead of emerging threats. KPMG FRM services and solutions can help agencies implement these critical capabilities to prevent, detect, and respond to fraud.

Contact us

To learn more: Visit.kpmg.us/fedrisk

Timothy Comello
Partner, Federal Advisory, KPMG LLP
T: 703-286-8580
E: tcomello@kpmg.com

Safa Khaleq
Managing Director, Federal Advisory, KPMG LLP
T: 571-512-8032
E: skhaleq@kpmg.com

John Iannacone
Director, Federal Advisory, KPMG LLP
T: 610-909-2178
E: jgiannacone@kpmg.com

Michelle McVicker
Manager, Federal Advisory, KPMG LLP
T: 703 453-7633
E: mmcvicker@kpmg.com

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

Learn about us: in | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.