Enhanced Government Financial Oversight

Reducing Fraud with AI and Metadata Analytics

Dr. Irakli Petriashvili

University of Georgia

IBM Center for
The Business
of Government

Enhanced Government Financial Oversight:
Reducing Fraud with AI and Metadata Analytics

Irakli Petriashvili, PhD
University of Georgia

MARCH 2026

IBM Center for
**The Business
of Government**

Table of Contents

AI-driven techniques can achieve high detection rates (of waste, fraud, and abuse in government), offering a path toward more accountable and effective oversight.

Foreword

Government financial oversight stands at an inflection point, enabled by artificial intelligence and other emerging technologies. As agencies manage increasingly complex digital financial systems, traditional audit methods—anchored in sampling, manual review, and documentation checks—can be supplemented by modern analytics approaches that help to address emerging risks to transparency, accountability, and public trust. Such strategies can more effectively safeguard taxpayer resources.

This report, *Enhanced Government Financial Oversight: Reducing Fraud with AI and Metadata Analytics*, by Dr. Irakli Petriashvili, Faculty Affiliate in the Transparency and Governance Center at Rutgers University (Newark), provides a timely and practical roadmap for enhancing the federal audit process. Drawing on deep analysis of government financial practices, reporting standards, and transaction data, the report highlights a critical need: current agency audit processes can still be limited by sampling-based audit approaches.

The report demonstrates the untapped power of supplementing audits with metadata—information automatically captured for every federal transaction. When paired with machine learning, metadata can enable auditors to analyze entire populations of transactions, uncover anomalies invisible to traditional methods, and detect fraud more accurately and at large scale. Experimental evidence presented by the author shows that AI-driven analytics outpace conventional sampling, revealing fraud patterns that would otherwise remain undetected.

The recommendations offered—including enabling metadata analysis as part of federal audit processes, launching AI pilot programs within agencies, and redefining oversight objectives to foster real-time protection for taxpayer funds—provide government leaders with a clear, actionable path forward. They reflect an evolution in government oversight, aligning audit practices with today's digital realities.

This report advances the IBM Center for The Business of Government's longstanding mission to strengthen public-sector performance through technology and innovation. Previous reports include: *Enhancing Government Payment Integrity: Leveraging AI and Other Emerging Technologies*, *A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding*, and *Government Procurement and Acquisition: Opportunities and Challenges Presented by Artificial Intelligence and Machine Learning*.

By embracing metadata intelligence and AI-enabled oversight, agencies can enhance audit and oversight processes to strengthen fraud detection and accountability—and in doing so, to build greater public trust in the stewardship of government resources.

Daniel J. Chenok
Executive Director
IBM Center for
The Business of Government
chenokd@us.ibm.com

Raafat Raafat
Associate Partner
Federal Finance and Supply
Chain Transformation, IBM
rraafat@us.ibm.com

Iman Aquil
Partner
Federal Finance
Transformation Practice, IBM
iman.a.aquil@us.ibm.com

Executive Summary

Federal financial audits can advance in practical impact through strategic transformation. Despite having strong oversight layers, existing financial audit design can be supplemented to enhance payment integrity in government spending.

The evidence reveals a stark contradiction. In 2024, 18 of 24 federal agencies received clean audit opinions, suggesting effective financial management. Yet the Government Accountability Office (GAO) estimates the federal government loses $233 billion to $521 billion annually to fraud. The contrast indicates significant opportunities to improve how financial audits relate to financial outcomes.

Federal financial audits are primarily designed to provide stakeholders, including Congress, the administration, and the public, with reasonable assurance that agency financial statements are accurate, complete, and presented fairly in accordance with U.S. Generally Accepted Accounting Principles (GAAP) for federal entities. Assurance is achieved through a series of manual audit procedures, such as reviewing supporting documentation, verifying account balances, and performing substantive testing on selected transactions. Because these procedures are labor-intensive and depend heavily on human oversight, auditors are limited in the number of transactions they can examine in detail. As a result, audits rely on sampling methods that cover only a fraction of total transactions. This reliance on manual processes and oversight creates practical constraints, often leaving potentially high risk or fraudulent payments outside the scope of review even when their aggregate value exceeds materiality thresholds. Addressing these limitations can allow evolving audit frameworks to better account for public resources and enhance fraud detection.

The analysis demonstrates that metadata—accompanying every government transaction—can provide powerful fraud detection capabilities. Applying machine learning to such metadata can bring orders of magnitude improvement in detecting fraudulent activity, relative to samplings methods used by most current audit processes.

By combining machine learning with metadata analytics, federal audit institutions can increase and improve analysis of entire populations of transactions, enabling them to enhance detection of anomalies and fraud patterns.

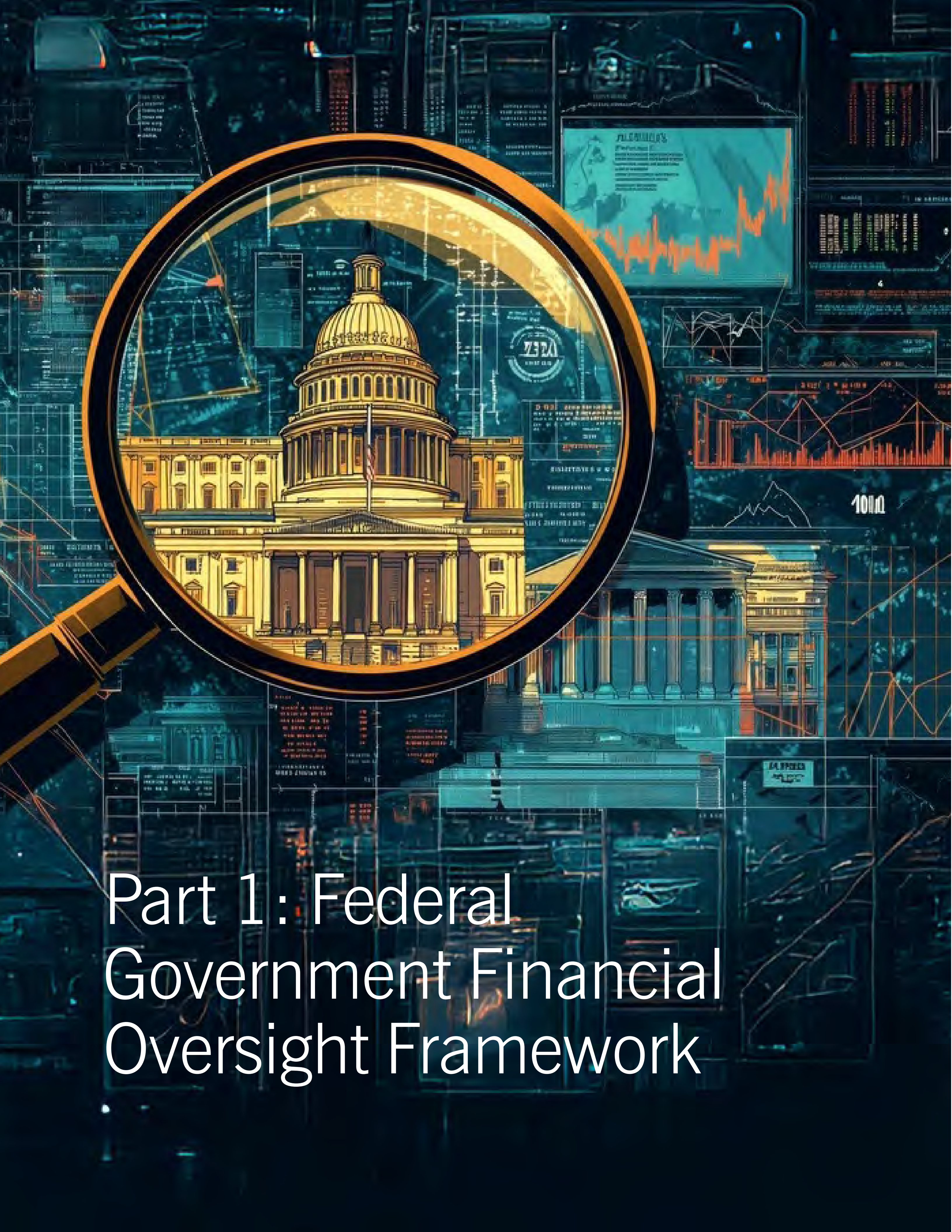
Introduction

Federal government financial oversight in the United States operates using a sophisticated framework, but one that has limitations. The framework combines executive branch oversight, congressional scrutiny, and independent audit institutions to safeguard public resources and promote fiscal accountability. However, current audit methodologies may not be sufficient to detect the scale of fraud threatening taxpayer funds.

The core issue lies in the difference between audit objectives and fraud detection capabilities. Federal financial audits, governed by the Financial Audit Manual (FAM) and Generally Accepted Government Auditing Standards (GAGAS), primarily assess whether financial statements fairly present agency financial positions according to accounting standards. While important for overall financial management and transparency goals, the objective does not directly address the protection of taxpayer funds.

This report addresses four fundamental questions: Do existing financial audit methodologies provide effective pathways for detecting fraud? What unique insights can be extracted to support fraud reduction from metadata embedded in public finance transactions? How can such metadata be operationalized by using machine learning algorithms within GAO and Offices of Inspectors General audit practices? Can the analysis of financial metadata significantly enhance fraud detection?

The results indicate that the current federal financial audit framework can change to improve government oversight of payment integrity. Existing audit methodologies often do not incorporate procedures to effectively use the metadata that accompanies each financial transaction, which can leave them short of adapting the latest trends and approaches from advancements in artificial intelligence and related technologies. Designed primarily for accounting and compliance purposes, these audits often do not address taxpayers’ broader interest in ensuring that public funds are safeguarded and not lost to waste, fraud, or abuse. AI-driven techniques can achieve high detection rates, offering a path toward more accountable and effective financial oversight.



Part 1: Federal Government Financial Oversight Framework

Federal Government Financial Oversight: Roles and Structure

Federal government financial oversight in the United States rests on a complex but carefully structured system of laws, institutions, and processes designed to ensure that taxpayer dollars are used lawfully, efficiently, and transparently.[1] At its core, this system aims to safeguard public resources, promote fiscal responsibility, and strengthen accountability to citizens.

Oversight is not the job of any single body, but the result of coordinated action among executive branch agencies, congressional committees, independent audit institutions, and statutory frameworks. Each plays a distinct, reinforcing role in managing, monitoring, and scrutinizing the flow and use of federal funds. The shared goal is not just compliance with legal requirements, but sustained trust in government stewardship of public resources.

At the center of the executive branch's financial management infrastructure is the Office of Management and Budget (OMB), which is organizationally located in the Executive Office of the President. OMB develops the federal budget, oversees its execution, and sets government-wide standards for financial reporting, internal controls, and performance management. Through its circulars and policy directives, OMB establishes consistent rules that federal agencies must follow, helping to unify fiscal practices across the government.

Working closely with OMB is the U.S. Department of the Treasury, whose Bureau of the Fiscal Service manages governmentwide accounting, payments, and debt collection. The Bureau ensures that the federal government's financial reporting is reliable, consistent, and timely. It serves as the technical backbone for collecting agency-level financial data and consolidating it into comprehensive reports that provide the clearest possible picture of the government's overall financial position.

Beyond the executive branch, the legislative branch plays a critical oversight role, with Congress itself serving as both the authorizer of spending and a central examiner of agency performance. Through its appropriations, budget, and oversight committees, Congress controls the flow of federal funds and sets expectations for how those funds are used. The Congressional Budget Office (CBO) supports this work by providing independent, nonpartisan analysis of fiscal and economic issues. Congressional hearings and investigations add further scrutiny, compelling agencies to justify their spending and demonstrate effective management.

Independent auditing and accountability are institutionalized most prominently in the work of the Government Accountability Office. As the nonpartisan audit arm of Congress, GAO provides objective analysis, program evaluations, and investigative findings to help lawmakers improve government performance and achieve savings. One of GAO's most important responsibilities is its annual audit of the U.S. government's consolidated financial statements; GAO also performs financial audits for certain agencies. This audit assesses whether those statements conform to U.S. generally accepted accounting principles, whether internal controls are effective, and whether laws and regulations are being followed.

Complementing GAO's governmentwide oversight are the Offices of Inspectors General (OIGs) embedded within each federal agency. Created under the Inspector General Act[2] of 1978 and reinforced by the Chief Financial Officers Act of 1990, OIGs are structured to operate inde-

[1] Stupak, Jeffrey M., Financial Stability Oversight Council (FSOC): Structure and Activities, CRS Report No. R45052, Congressional Research Service, February 12, 2018.

[2] Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified as amended in scattered sections of 5 U.S.C. app.); Chief Financial Officers Act of 1990, Pub. L. No. 101-576, 104 Stat. 2838 (codified in 31 U.S.C. §§ 901–903); U.S. Congressional Research Service, Statutory Inspectors General in the Federal Government: A Primer, CRS Report No. R45450, updated August 15, 2019.

pendently while remaining part of their parent agencies. Their mission is to detect and prevent fraud, waste, and abuse, offering an internal mechanism of accountability. IGs report to both their agency heads and to Congress, creating a dual reporting line that reinforces their independence and effectiveness.

The CFO Act itself was transformative in strengthening the federal financial oversight structure. By establishing Chief Financial Officer positions in major agencies and creating the Deputy Director for Management at OMB, the Act mandated standardized financial management practices, including the production of annual audited financial statements and formal evaluations of internal controls. This legislation institutionalized the expectation that federal agencies must demonstrate transparency, accuracy, and stewardship in their financial operations.

Despite the encouraging fact that, in fiscal year 2024,[3] 18 of 24 CFO Act agencies achieved a clean, unqualified audit opinion, significant concerns about fraud and financial abuse remain deeply embedded within the federal landscape.

A clean audit opinion reflects that, based on the procedures performed, no material misstatements were detected, and the financial statements meet these standards. However, a clean audit does not guarantee the absence of fraud or misuse of funds. The reasonable assurance provided by clean audits is limited by the scope of manual audit functions, such as reviewing documentation and sampling transactions, which means only a small fraction of total activity is examined in detail. As a result, high-risk or fraudulent payments may remain undetected, underscoring the need for evolving audit frameworks that go beyond existing approaches to better protect public resources.

Yet even this picture may not represent the full scope of fraud and financial mismanagement across the federal landscape. As the 2024 Report to the Nations[4] by the Association of Certified Fraud Examiners (ACFE) illustrates, external audits are not the cornerstone of anti-fraud controls, especially in the U.S. According to the report, the external audit role as anti-fraud control is only 73 percent effective in the United States, a figure that trails well behind Southern Asia (95 percent), Eastern Europe and Western/Central Asia (94 percent), and Western Europe (90 percent). This disparity suggests that although external audits are common in U.S. federal oversight, their deployment as a deliberate anti-fraud measure remains comparatively limited.

This reliance on reactive, human-driven reporting mechanisms over systematic, data-enabled detection strategies reveals an opportunity to close gaps in the current audit-based approach to fraud prevention.

The same ACFE report indicates that external audits in the U.S. play a comparatively weaker role in detecting fraud relative to other global regions. Importantly, the ACFE data highlights how fraud is discovered in practice. Across 1,921 cases studied worldwide, tips, especially from whistleblowers, emerged as the single most common initial detection method, responsible for 43 percent of cases globally and 35 percent in the United States. By stark contrast, external financial audits accounted for only 3 percent of initial detections, both globally and domestically. This raises serious questions about whether conventional audits alone can deliver the level of oversight needed to identify and disrupt sophisticated, hidden, or distributed fraud schemes. Expanding the audit process to add anti-fraud analysis, as demonstrated by the analysis later in this report, could enhance the value of internal controls.

[3] U.S. Government Accountability Office, Federal Financial Accountability, GAO-25-107753, March 11, 2025; U.S. Department of the Treasury, Financial Report of the United States Government, Fiscal Year 2024, Independent Auditor's Report, January 8, 2025.

[4] Association of Certified Fraud Examiners, Occupational Fraud 2024: A Report to the Nations, 13th ed. (Austin, TX: ACFE, March 2024).

These realities raise questions about the future of federal financial oversight. Are current audit methodologies optimized to detect fraud, waste, and inefficiency at the scale of the U.S. government's vast and complex financial operations? And are federal agencies and oversight bodies effectively leveraging the wealth of transactional data now available to them?

These questions are explored within the framework of federal financial audits mandated under the CFO Act of 1990, which established standardized benchmarks for financial reporting and accountability across executive agencies.[5] As one of the most widespread and regulated forms of oversight, federal financial audits are governed by the Financial Audit Manual (FAM) and guided by Generally Accepted Government Auditing Standards (GAGAS). That said, it should be noted that the Federal Government Financial Oversight framework covers more than financial statement audits (FSAs). The current federal FSAs are large and complex and have a specific purpose (i.e., to provide **reasonable assurance** that the statements are free from **material misstatement**). The government has supplemental agency and OIG responsibilities identified in OMB Circular A-123, the Fraud Reduction and Data Analytics Act of 2015, and similar authorities. Although this paper focuses on the audit process, its findings may apply to the use of AI for the analysis of fraud detection and reduction in other processes required by law and policy.

Institutional Roles in U.S. Federal Financial Audits: Comparing GAO and OIG in Practice

Financial audits are a cornerstone of public accountability in the United States federal government, serving as a critical mechanism to ensure that taxpayer dollars are used lawfully, efficiently, and transparently.[6] These audits provide independent assurance about the accuracy of agencies' financial statements, the effectiveness of internal controls, and compliance with applicable financial laws and regulations. Underpinning this work is a rigorous methodological[7] foundation rooted in the GAGAS and the FAM. These frameworks shape how audits are executed across the federal landscape, primarily by two distinct but complementary institutional entities: the Government Accountability Office and the Offices of Inspectors General.

While both GAO and the OIGs operate under the same professional auditing standards, their roles, responsibilities, and practices differ significantly in scope, authority, and operational context. GAO functions as an independent, nonpartisan agency within the legislative branch, and is the primary audit institution responsible for governmentwide financial oversight; its mandate includes evaluating the consolidated financial position of the entire federal government. By contrast, OIGs are independent units embedded within individual executive branch agencies, tasked with ensuring agency-level financial accountability while maintaining autonomy from agency management.

GAGAS, commonly known as the Yellow Book, establishes comprehensive standards governing all phases of the federal audit process, including planning, fieldwork, and reporting. It emphasizes key principles such as independence, objectivity, professional competence, and the use of evidence-based analysis. By enforcing a uniform set of expectations, GAGAS promotes methodological consistency and professional integrity across all federal audit institutions.

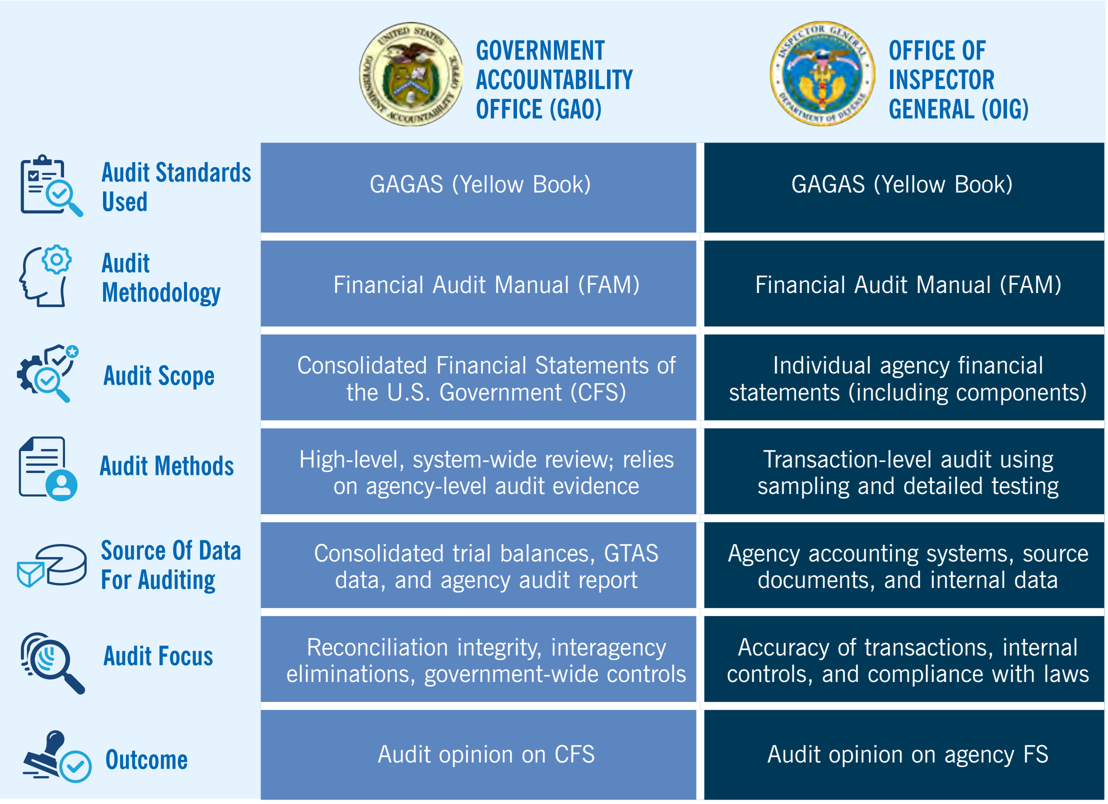
[5] https://www.cio.gov/handbook/it-laws/cfo-act.

[6] U.S. Government Accountability Office. Federal Financial Management: Critical Accountability and Fiscal Stewardship Challenges Facing Our Nation. Testimony before the U.S. Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security. GAO-07-542T. Washington, DC: U.S. Government Accountability Office, March 1, 2007.

[7] U.S. Government Accountability Office, Government Auditing Standards (commonly known as GAGAS or the Yellow Book), GAO-24-106786, February 2024; U.S. Government Accountability Office and Council of the Inspectors General on Integrity and Efficiency (CIGIE), Financial Audit Manual (FAM), Vol. 1, June 2024.

Translating these standards into practical audit procedures is the purview of the FAM. Jointly developed by GAO and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the FAM provides detailed, standardized guidance for executing financial statement audits within the federal context. It ensures that agencies and auditors apply GAGAS consistently while adapting procedures to their specific audit environments. The FAM outlines a structured approach to the entire audit lifecycle, from risk assessment and audit strategy design to internal control testing, account verification, and issuance of audit opinions. These procedures are designed to comply with statutory requirements, including the Chief Financial Officers (CFO) Act[8] of 1990, the Federal Financial Management Improvement Act (FFMIA), and the Payment Integrity Information Act (PIIA). These statutes have fundamentally shaped expectations for transparency, accountability, and high-quality financial management in federal agencies. See details in Figure 1.

Figure 1: Institutional Roles in U.S. Federal Financial Audits: GAO and OIG



	GOVERNMENT ACCOUNTABILITY OFFICE (GAO)	OFFICE OF INSPECTOR GENERAL (OIG)
Audit Standards Used	GAGAS (Yellow Book)	GAGAS (Yellow Book)
Audit Methodology	Financial Audit Manual (FAM)	Financial Audit Manual (FAM)
Audit Scope	Consolidated Financial Statements of the U.S. Government (CFS)	Individual agency financial statements (including components)
Audit Methods	High-level, system-wide review; relies on agency-level audit evidence	Transaction-level audit using sampling and detailed testing
Source Of Data For Auditing	Consolidated trial balances, GTAS data, and agency audit report	Agency accounting systems, source documents, and internal data
Audit Focus	Reconciliation integrity, interagency eliminations, government-wide controls	Accuracy of transactions, internal controls, and compliance with laws
Outcome	Audit opinion on CFS	Audit opinion on agency FS

Source: Authors original work (all Figures in this report represent the author's original work, unless otherwise cited)

Financial Statement Preparation and Audit Execution in the Federal Government: The Operational Reality Within CFO Act Agencies

Agencies governed by the Chief Financial Officers Act[9] of 1990 are legally mandated to produce annual, audited financial statements. These entities include many of the federal government's largest, most complex, and resource-intensive components. As such, the audit process

[8] Chief Financial Officers Act of 1990, Pub. L. No. 101-576, 104 Stat. 2838 (codified at 31 U.S.C. §§ 901–903); Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, div. A, title I, § 101(f) [title VIII], 110 Stat. 3009-389 (codified at 31 U.S.C. § 3512 note); Payment Integrity Information Act of 2019, Pub. L. No. 116-117, 134 Stat. 113 (codified at 31 U.S.C. §§ 3351–3358).

[9] Chief Financial Officers Act of 1990, Pub. L. No. 101-576, § 303, 104 Stat. 2838, 2849 (codified at 31 U.S.C. § 3515).

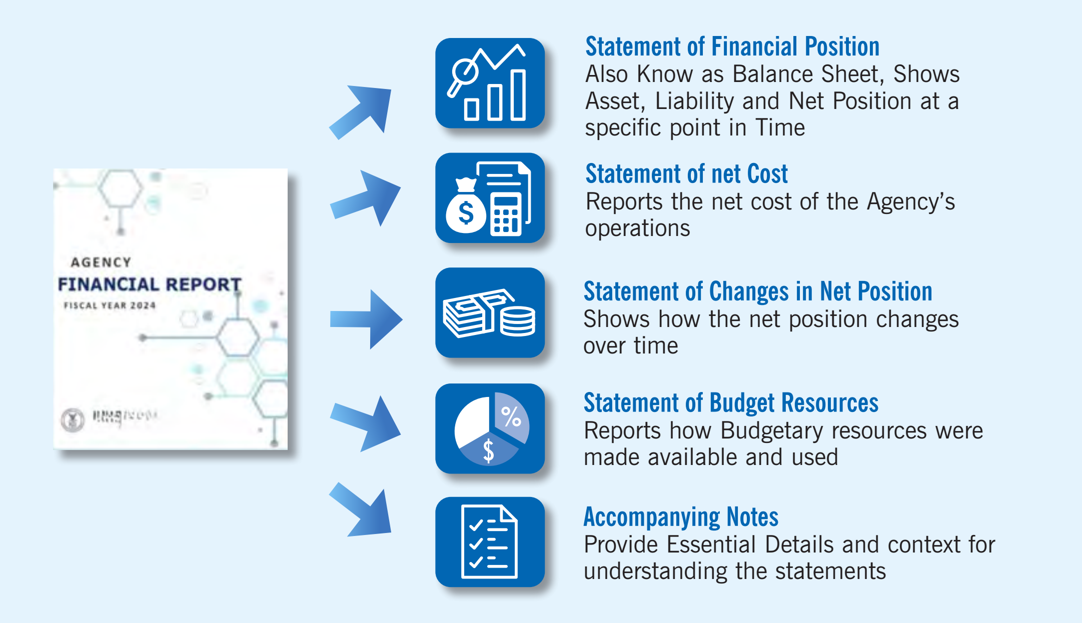
in these agencies operates at a scale that requires both strict methodological discipline and practical flexibility that accommodates real-world operational complexity.

Generally, the financial audit process for CFO Act agencies begins internally—with the core responsibility for preparing accurate, complete, and compliant financial records resting with the agencies themselves (as noted previously, GAO does perform audits of certain agencies (such as, IRS, SEC). Throughout the fiscal year, agencies process and record millions of financial transactions that cover payroll, procurement, grants, travel reimbursements, and other operational expenditures. These transactions are managed using enterprise resource planning (ERP) or other federal financial management systems designed to ensure adherence to federal accounting principles.

Each transaction is recorded in accordance with standards[10] set by the Federal Accounting Standards Advisory Board (FASAB) and is classified using the U.S. Standard General Ledger (USSGL). To ensure traceability and data integrity, every transaction carries a rich set of metadata fields, including Treasury Account Symbols (TAS), budget object class codes, program activity codes, vendor identifiers, and disbursement dates. This metadata structure enables agencies to accurately classify, reconcile, and report financial activities in a way that supports both internal management and external accountability.

As the fiscal year concludes, agencies consolidate these individual transactions to produce trial balances and prepare their annual financial statements. This consolidation process involves making necessary accruals, performing year-end adjustments, and conducting thorough internal reconciliations to ensure data accuracy and compliance with federal reporting requirements. The resulting financial statements typically include five core components. See Figure 2.

Figure 2: Financial Statement Components



Statement of Financial Position
Also Know as Balance Sheet, Shows Asset, Liability and Net Position at a specific point in Time

Statement of net Cost
Reports the net cost of the Agency's operations

Statement of Changes in Net Position
Shows how the net position changes over time

Statement of Budget Resources
Reports how Budgetary resources were made available and used

Accompanying Notes
Provide Essential Details and context for understanding the statements

[10] Federal Accounting Standards Advisory Board, *The Federal Accounting Standards Advisory Board Handbook of Federal Accounting Standards and Other Pronouncements, as Amended (FASAB Handbook)*, June 2024; U.S. Department of the Treasury, Bureau of the Fiscal Service, *U.S. Standard General Ledger: 2024 Accounting Handbook*, June 2024.

These financial statements are developed in full compliance with OMB Circular A-136, which sets forth the federal government's financial reporting requirements and ensures a standardized approach across agencies. Once finalized, these statements serve two critical purposes: they are submitted *internally* to the agency's OIG for audit and *externally* to the Department of the Treasury for inclusion in the governmentwide consolidated financial reporting process.

Financial Statement Audit Process General level—Defense IG Case Study

The use case used for this paper—from the Department of Defense, now referred to as the Department of War (DOW)—illustrates how federal agencies prepare consolidated financial statements and conduct inspector general financial audits. This case demonstrates, in practical terms, the complete audit process within a single agency context, from financial statement preparation through Office of Inspector General audit execution.

The focus on the Pentagon is both deliberate and instructive for government financial managers. As the largest federal agency governed by the Chief Financial Officers Act of 1990, DOW represents a uniquely complex and high-stakes environment for financial management and oversight. Its vast budget, procurement and operations scale, and sheer volume of transactions make it highly relevant for understanding the challenges and nuances of federally mandated financial accountability. The Department has also been identified as a high-risk area, given long-standing internal control weaknesses and significant audit readiness challenges, making it an ideal example for illustrating both the rigor and limitations of the federal audit process. In addition, the Department's audit status represents a factor in GAO's inability to offer an opinion on the audit statement for the government as a whole.

DOW prepares its agency-wide consolidated financial statements through a process that requires collecting, standardizing, and consolidating financial data from dozens of subordinate Components. Each Component's financial data must comply with federal accounting principles, including classification using the U.S. Standard General Ledger, and must follow the reporting requirements laid out in OMB Circular A-136. The resulting consolidated financial statements aim to provide a complete and accurate picture of the Department's financial position, performance, and budgetary resources.

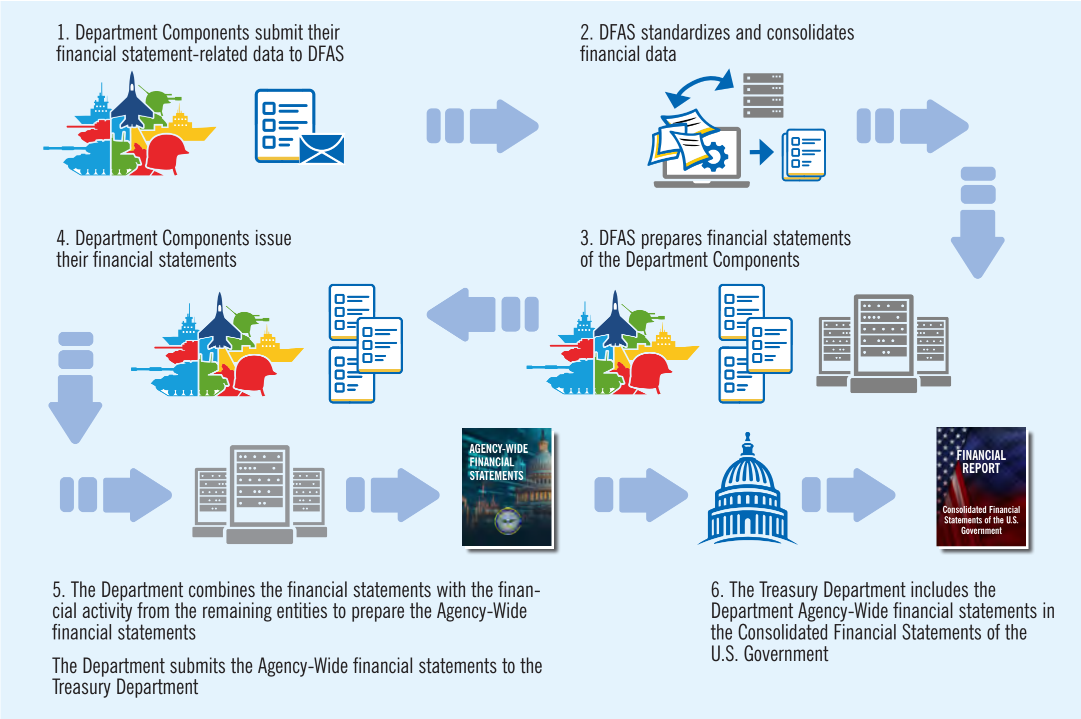
As illustrated in Figure 3, the Pentagon consolidates financial activity from 62 distinct entities, creating a complex web of data that defines manual verification. Whether these components issue stand-alone reports or are integrated directly by the Defense Finance and Accounting Service (DFAS),[11] the sheer volume of this consolidation process creates the specific 'blind spots' where fraud hides.

Once finalized, these consolidated financial statements, and all required supplemental details, are submitted to the U.S. Department of the Treasury. Treasury uses this information to help compile the Consolidated Financial Statements of the U.S. Government.

Whether a DOW Component issues a stand-alone statement or is included directly in the consolidated report depends largely on the materiality of its financial activity. Entities with larger or more significant financial impact are more likely to have separate audited reports to ensure transparency and accountability.

[11] U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller), Agency Financial Report, Fiscal Year 2024, November 2024.

Figure 3: Key Steps for Preparing the Pentagon Financial Statements


1. Department Components submit their financial statement-related data to DFAS
2. DFAS standardizes and consolidates financial data
3. DFAS prepares financial statements of the Department Components
4. Department Components issue their financial statements
AGENCY-WIDE FINANCIAL STATEMENTS
FINANCIAL REPORT
Consolidated Financial Statements of the U.S. Government
5. The Department combines the financial statements with the financial activity from the remaining entities to prepare the Agency-Wide financial statements
The Department submits the Agency-Wide financial statements to the Treasury Department
6. The Treasury Department includes the Department Agency-Wide financial statements in the Consolidated Financial Statements of the U.S. Government

Source: The DOW OIG

Following the preparation and consolidation of its agency-wide financial statements, the Pentagon undertakes a full-scope financial audit in compliance with the requirements of the Chief Financial Officers Act of 1990. The audit is executed under the direction of the Office of Inspector General, which maintains oversight authority but delegates most fieldwork to Independent Public Accounting (IPA) firms contracted to perform audits of individual reporting Components.

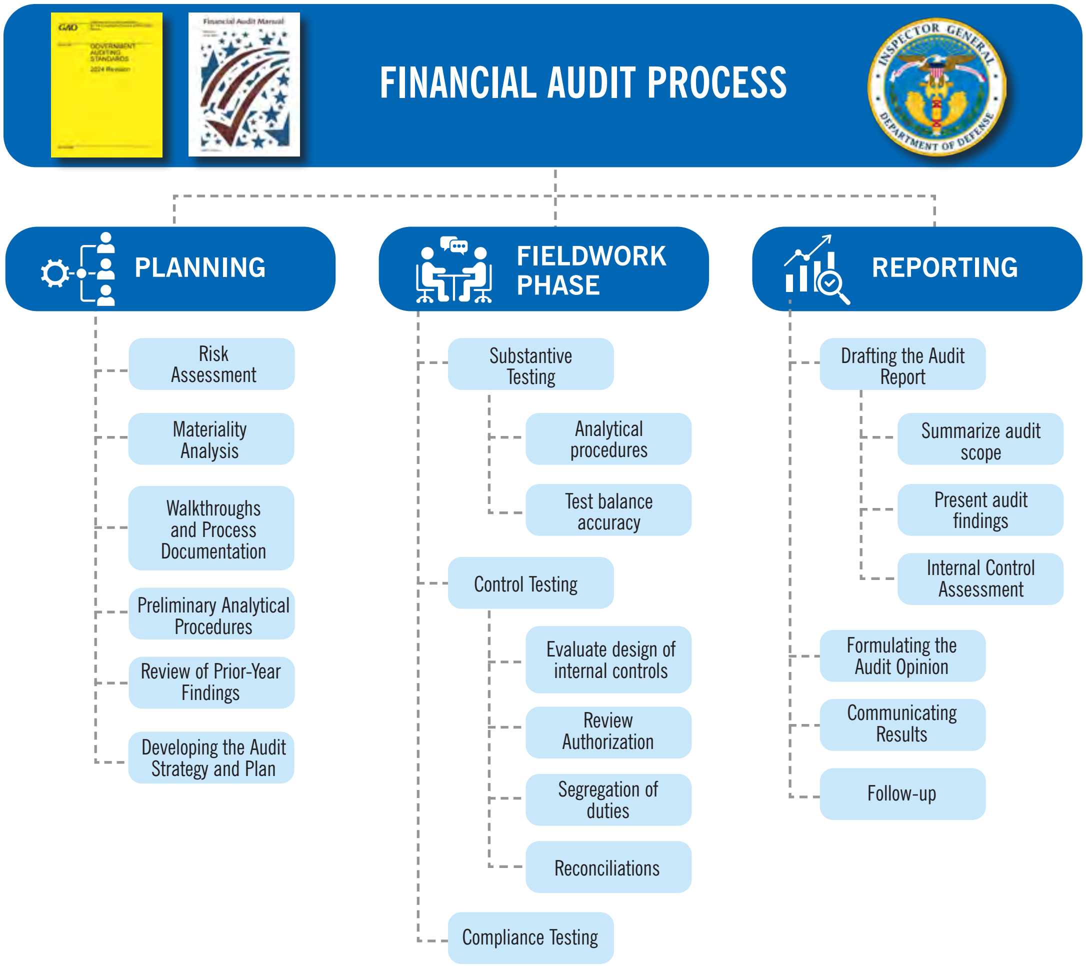
All audit activities are conducted in accordance with the Generally Accepted Government Auditing Standards, commonly known as the "Yellow Book," and Financial Audit Manual. GAGAS establishes uniform requirements for planning, evidence collection, internal control testing, and reporting in government audits.[12] At the agency level, the Pentagon adheres to OMB Bulletin[13] No. 24-01, which outlines specific financial reporting and audit submission requirements for federal entities.

Once the Department-wide financial statements are finalized by the Defense Finance and Accounting Service (DFAS) based on both audited and unaudited inputs, the agency OIG consolidates audit findings and conducts a top-down review to issue an audit opinion on the agency-wide financial position. For detailed financial audit procedures, see Figure 4.

[12] U.S. Government Accountability Office, *Government Auditing Standards* (commonly known as the "Yellow Book"), GAO-24-106786, February 2024; U.S. Government Accountability Office and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual (FAM)*, Vol. 1, June 2024

[13] U.S. Office of Management and Budget, OMB Bulletin No. 24-01: Audit Requirements for Federal Financial Statements, August 2023.

Figure 4: Financial Audit Process According FAM and GAGAS

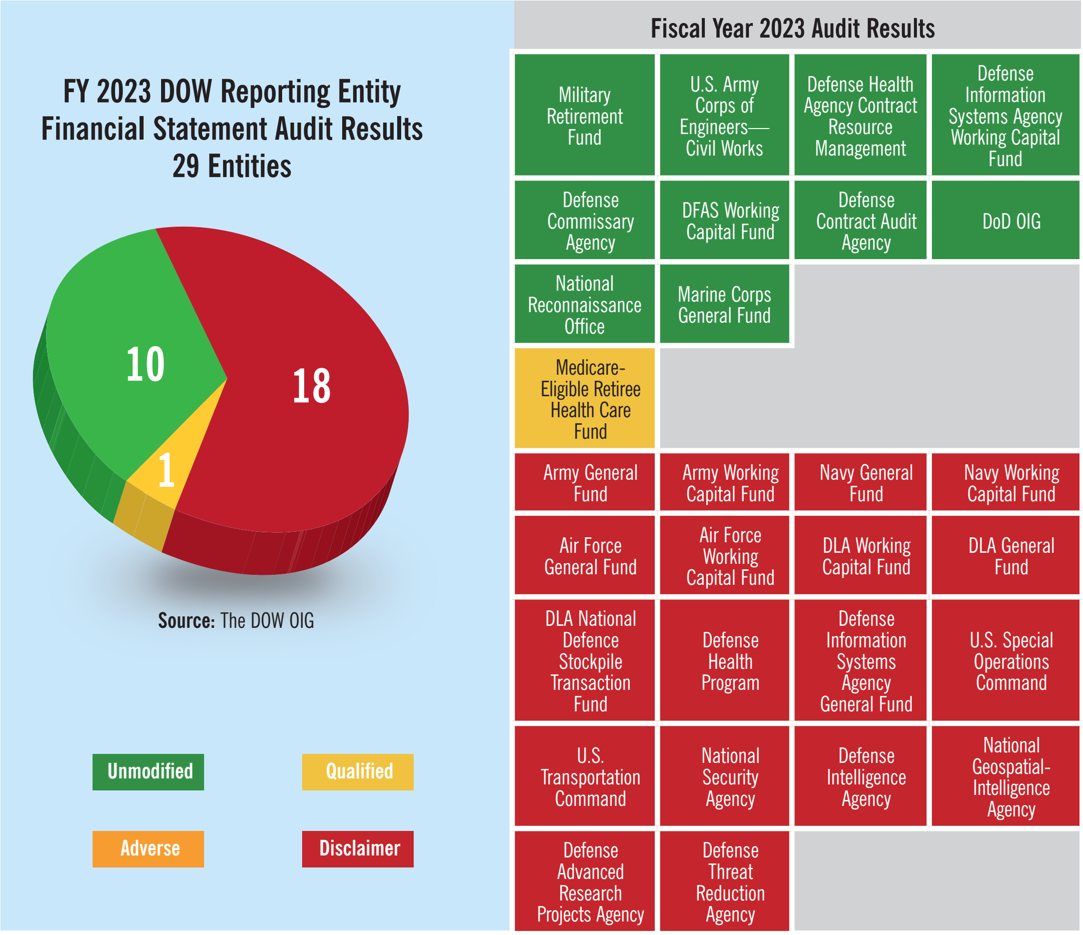


The core of the federal financial audit process lies in the fieldwork phase, particularly the execution of substantive procedures. During this stage, auditors gather the most critical evidence to support their opinion on the accuracy of financial statements and to uncover potential fraud. Substantive procedures are composed of two main techniques: tests of details and substantive analytical procedures. Together, they are designed to verify the accuracy, completeness, and validity of reported transactions.

In practice, auditors review invoices, examine contracts, recalculate financial figures, and confirm account balances with third parties. These steps establish that the transactions recorded by the agency are legitimate, properly authorized, and compliant with applicable financial regulations.

The DOW OIG issues an audit opinion to determine whether financial statements are fairly presented, to identify material weaknesses in internal controls, and to assess compliance with applicable laws. The process highlights the importance of collecting sufficient and appropriate audit evidence. Based on this evidence, the OIG may issue one of four types of audit opinions. A clean (unmodified) opinion indicates that the financial statements are presented fairly in all material respects. An adverse opinion signals that the statements do not accurately reflect the entity's financial position. However, even a clean opinion does not guarantee the absence of fraud or abuse; it simply means that no material misstatements were detected based on the procedures performed. See audit opinions[14] by Department components in Figure 5.

Figure 5: DOW Financial Audit Opinions by Each Agency



Source: The DOW OIG

Fiscal Year 2023 Audit Results

🟩 Military Retirement Fund	🟩 U.S. Army Corps of Engineers—Civil Works	🟩 Defense Health Agency Contract Resource Management	🟩 Defense Information Systems Agency Working Capital Fund
🟩 Defense Commissary Agency	🟩 DFAS Working Capital Fund	🟩 Defense Contract Audit Agency	🟩 DoD OIG
🟩 National Reconnaissance Office	🟩 Marine Corps General Fund		
🟨 Medicare-Eligible Retiree Health Care Fund			
🟥 Army General Fund	🟥 Army Working Capital Fund	🟥 Navy General Fund	🟥 Navy Working Capital Fund
🟥 Air Force General Fund	🟥 Air Force Working Capital Fund	🟥 DLA Working Capital Fund	🟥 DLA General Fund
🟥 DLA National Defence Stockpile Transaction Fund	🟥 Defense Health Program	🟥 Defense Information Systems Agency General Fund	🟥 U.S. Special Operations Command
🟥 U.S. Transportation Command	🟥 National Security Agency	🟥 Defense Intelligence Agency	🟥 National Geospatial-Intelligence Agency
🟥 Defense Advanced Research Projects Agency	🟥 Defense Threat Reduction Agency		

Consolidated Financial Statement Audit Process Government Accountability Office GAO—Process Snapshot

The U.S. Department of the Treasury's Bureau of the Fiscal Service, in coordination[15] with the Office of Management and Budget, prepares the Consolidated Financial Statement (CFS) by aggregating financial information from across the federal government, including the 24 CFO Act agencies and other entities. These individual agencies are first responsible for submitting their year-end audited financial statements. Most CFO Act agencies undergo audits either by their respective Offices of Inspectors General or by Independent Public Accounting firms. Treasury then compiles this data, using the Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) as a central repository. This stage involves:

[14] U.S. Department of Defense (now referred to as DOW), Office of the Under Secretary of Defense (Comptroller), Agency Financial Report, Fiscal Year 2024, November 2024.

[15] U.S. Department of the Treasury, Bureau of the Fiscal Service, Financial Report of the United States Government, Fiscal Year 2024, January 2025; U.S. Office of Management and Budget, OMB Circular No. A-136: Financial Reporting Requirements, August 2023.

- Submission of adjusted trial balances and footnote data from each agency
- Elimination of intragovernmental transactions and balances
- Standardization of accounting classifications under the U.S. Standard General Ledger

The final product is the Financial Report[16] of the United States Government, which includes four principal statements:

1. The Statement of Net Cost
2. The Statement of Operations and Changes in Net Position
3. The Balance Sheet
4. The Statement of Budgetary Resources

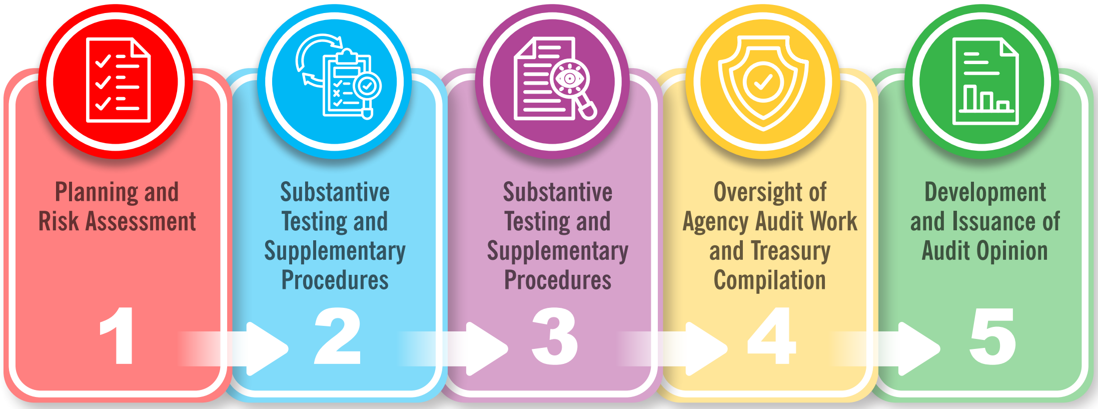
This report is accompanied by extensive notes, required supplementary information, and an overview of the federal government's long-term fiscal outlook.

The Government Accountability Office is statutorily responsible for auditing the consolidated financial statements of the U.S. Government, pursuant to the Government Management Reform Act[17] of 1994. This audit provides the public, Congress, and executive leadership with an independent assessment of the reliability, completeness, and accuracy of the federal government's financial position. In general, GAO[18] does not perform detailed audits of each federal entity. Instead, it relies on agency-level audit results, particularly those from the 24 CFO Act agencies. For these, GAO reviews:

- The audit opinions issued by OIGs or Independent Public Accounting firms
- Reports on internal control weaknesses, and notes on noncompliance with laws and regulations.

Using this information, GAO performs supplementary procedures as needed, particularly when audit evidence is insufficient or agencies have not audited their financial statements. GAO's consolidated audit work includes the following phases. See Figure 6.

Figure 6: Financial Audit Process Conducted by GAO


Planning and Risk Assessment
1
Substantive Testing and Supplementary Procedures
2
Substantive Testing and Supplementary Procedures
3
Oversight of Agency Audit Work and Treasury Compilation
4
Development and Issuance of Audit Opinion
5

[16] U.S. Department of the Treasury, Bureau of the Fiscal Service, Financial Report of the United States Government, Fiscal Year 2024, January 2025.

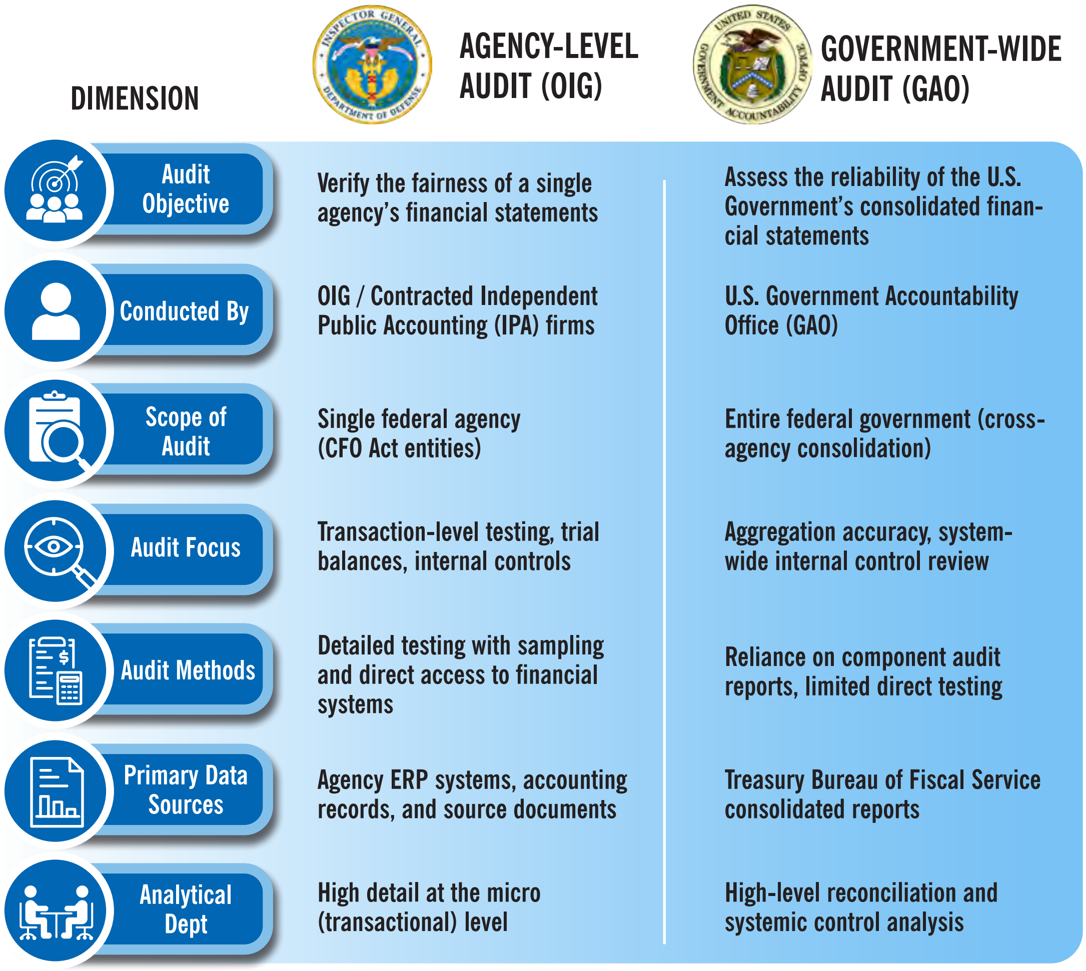
[17] Government Management Reform Act of 1994, Pub. L. No. 103-356, § 405, 108 Stat. 3410, 3423 (codified at 31 U.S.C. § 331(e)).

[18] U.S. Government Accountability Office, Financial Audit: Fiscal Year 2024 Financial Report of the United States Government, GAO-25-105618, January 2025.

GAO's audit execution process relies heavily on the foundation laid by the OIGs. It begins with an assessment of whether the underlying agency audits are reliable, based on the audit opinions issued, internal control findings, and identified limitations. Where agency financials are un-auditable or where material weaknesses are pervasive, GAO may perform targeted procedures or disclaim an opinion entirely. GAO also audits the Treasury's consolidation methodology itself, evaluating whether eliminations are valid, inter-agency balances reconcile, and whether the overall structure produces a materially accurate portrait of the government's financial position.

Federal financial audits are executed through a layered, interdependent model that depends on the integrity of each component to deliver credible oversight at the macro level. Both audit processes are indispensable, but their design serves distinct purposes. See Figure 7.

Figure 7: Financial Audit Execution Process OIG and GAO Level



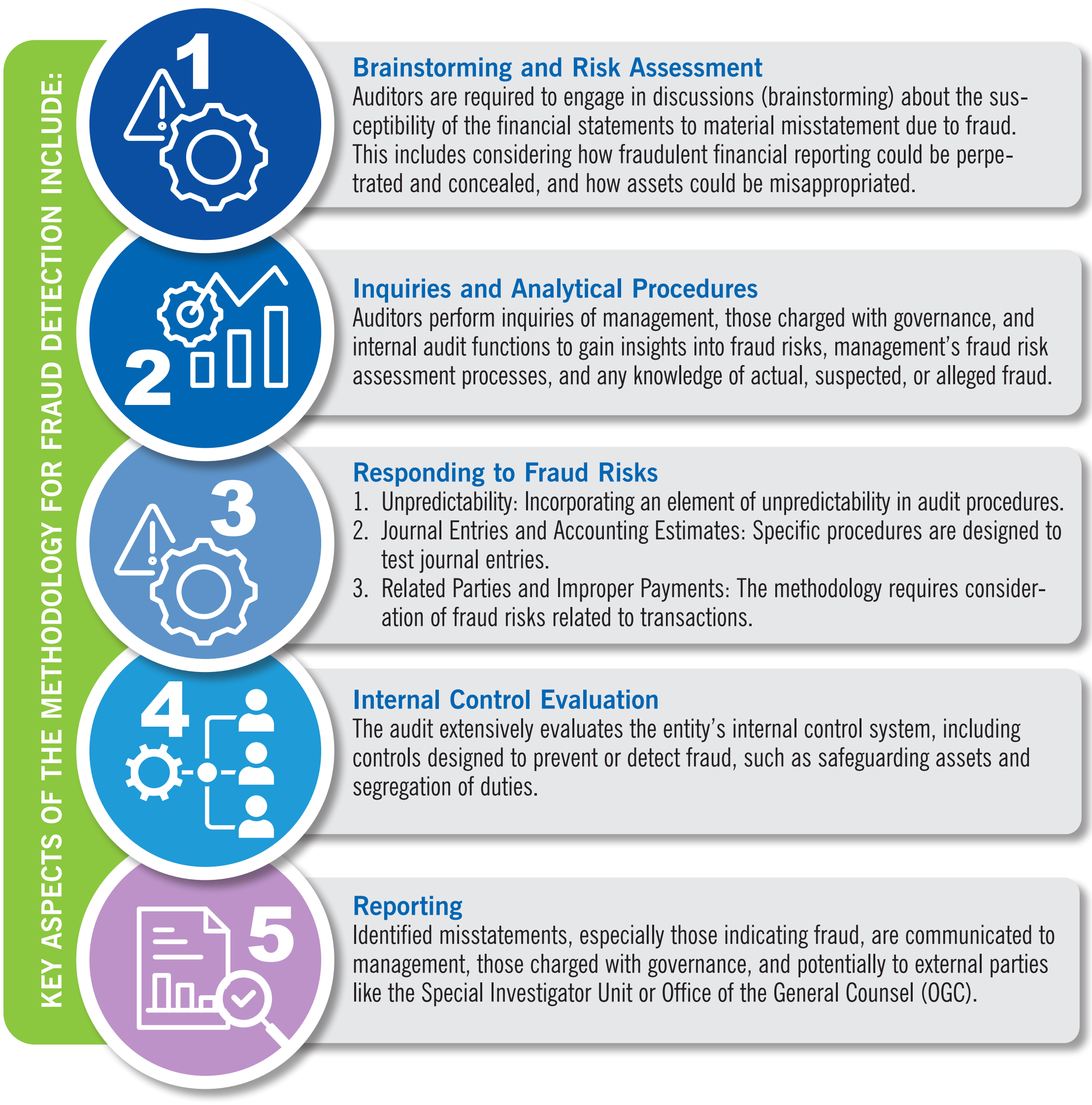
DIMENSION	AGENCY-LEVEL AUDIT (OIG)	GOVERNMENT-WIDE AUDIT (GAO)
Audit Objective	Verify the fairness of a single agency's financial statements	Assess the reliability of the U.S. Government's consolidated financial statements
Conducted By	OIG / Contracted Independent Public Accounting (IPA) firms	U.S. Government Accountability Office (GAO)
Scope of Audit	Single federal agency (CFO Act entities)	Entire federal government (cross-agency consolidation)
Audit Focus	Transaction-level testing, trial balances, internal controls	Aggregation accuracy, system-wide internal control review
Audit Methods	Detailed testing with sampling and direct access to financial systems	Reliance on component audit reports, limited direct testing
Primary Data Sources	Agency ERP systems, accounting records, and source documents	Treasury Bureau of Fiscal Service consolidated reports
Analytical Dept	High detail at the micro (transactional) level	High-level reconciliation and systemic control analysis

Methodological Analysis for Fraud Detection in Financial Audit—Actions, Procedures and limitations

While the primary goal of federal financial audits is to provide assurance on the fairness of financial statements, both FAM and GAGAS emphasize the auditor's responsibility to assess and respond to fraud risks throughout the audit lifecycle.

Below is provided a synthesized view of the methodology,[19] emphasizing critical actions to detect fraud such as risk identification, professional skepticism, internal control testing, journal entry analysis, and the role of auditor judgment. Figures 8 and 9 illustrate required actions and procedures within federal financial audit, to embed fraud-related considerations within financial audit process.

Figure 8: Actions Defined from Financial Audit Manual (FAM) for Fraud Detection



KEY ASPECTS OF THE METHODOLOGY FOR FRAUD DETECTION INCLUDE:

Brainstorming and Risk Assessment
Auditors are required to engage in discussions (brainstorming) about the susceptibility of the financial statements to material misstatement due to fraud. This includes considering how fraudulent financial reporting could be perpetrated and concealed, and how assets could be misappropriated.

Inquiries and Analytical Procedures
Auditors perform inquiries of management, those charged with governance, and internal audit functions to gain insights into fraud risks, management's fraud risk assessment processes, and any knowledge of actual, suspected, or alleged fraud.

Responding to Fraud Risks

1. Unpredictability: Incorporating an element of unpredictability in audit procedures.
2. Journal Entries and Accounting Estimates: Specific procedures are designed to test journal entries.
3. Related Parties and Improper Payments: The methodology requires consideration of fraud risks related to transactions.

Internal Control Evaluation
The audit extensively evaluates the entity's internal control system, including controls designed to prevent or detect fraud, such as safeguarding assets and segregation of duties.

Reporting
Identified misstatements, especially those indicating fraud, are communicated to management, those charged with governance, and potentially to external parties like the Special Investigator Unit or Office of the General Counsel (OGC).

[19] U.S. Government Accountability Office, *Government Auditing Standards* (commonly known as the "Yellow Book"), GAO-24-106786, February 2024; U.S. Government Accountability Office and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual (FAM)*, Vol. 1, June 2024.

Figure 9: Procedures from Financial Audit Manual to Respond to Fraud

AUDITOR RESPONSIBILITY FOR EXECUTING PROCEDURES RELATED TO FRAUD DETECTION				
Audit Phase	**Audit procedures1**	**Audit procedures 2**	**Audit procedures 3**	**Audit procedures 4**
Planning	Identify and Assess Risks: Auditor is responsible for identifying and assessing risks of material misstatement due to fraud at both the financial statement and assertion levels.	Understand Internal Control: Auditors gain an understanding of the entity's internal control, including how it is designed to prevent and detect fraud, and how IT affects these controls.	**Inquiries:** Auditors are responsible for inquiring of management, those charged with governance, and internal audit about their knowledge of fraud and their fraud risk assessment processes.	Documentation of identified fraud risks, the brainstorming discussions, and the overall responses to such risks is required.
Internal Control Evaluation	Understand and Evaluate Controls: Auditors are responsible for understanding the design of relevant control activities.	Test Controls: If controls are suitably designed and implemented, auditors perform tests of their operating effectiveness.	IS Controls Auditor Involvement: An IS controls auditor (a specialist in information technology systems, general controls, applications, and information security) is typically involved in understanding, planning, directing, and performing audit procedures related to assessing IS controls, which are crucial for detecting and preventing IT-related fraud.	
Field Work—Testing	Design and Perform Further Procedures: Auditors design and perform substantive and compliance procedures that are responsive to the assessed risks of material misstatement, including those due to fraud. This includes incorporating an element of unpredictability in selecting items for testing.		Specialist Consultation: An audit sampling specialist is generally consulted for assistance in designing and evaluating audit samples, especially when statistical sampling methods (like MUS or classical variables sampling) are used for substantive tests, which can enhance fraud detection by allowing for defensible projections.	
Reporting	Evaluate Misstatements: Auditors evaluate whether detected misstatements, individually or in aggregate, indicate fraud.	Communication: Significant findings and issues, especially those related to fraud, are communicated to management and those charged with governance.	External Reporting: If an instance of fraud is identified or suspected, the auditor, in consultation with the audit director, determines whether to seek assistance from the Special Investigator Unit or OGC, and whether there is a responsibility to report to parties outside the entity, potentially overriding confidentiality in certain circumstances. The auditor's report is modified if fraud results in a material misstatement.	

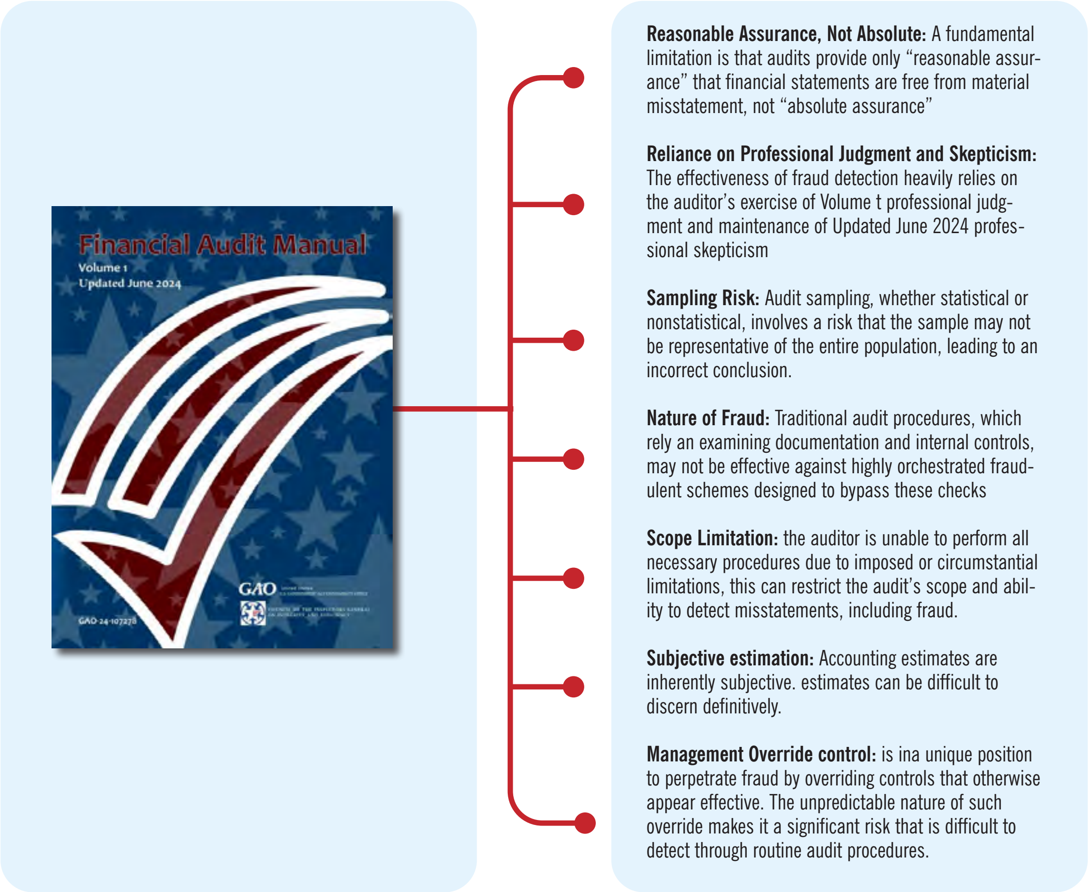
Source: The Financial Audit manual (FAM) U.S GAO

Besides actions and procedures to respond to fraud in financial audit, the Financial Audit Manual explicitly acknowledges a critical limitation: it is designed to provide reasonable assurance, not absolute assurance, that financial statements are free from material misstatement due to fraud or error. This distinction is significant. Even the most carefully planned and executed audits carry an inherent risk that certain misstatements may go undetected. The likelihood of overlooking fraud is particularly elevated compared to detecting errors, due to the deliberate nature of fraudulent acts such as collusion, forgery, intentional omissions, or management override of controls . By adding a forward-looking fraud analytics process to complement current financial reporting pathways, agencies can improve detection and reporting in data used for Congressional and public reports.

Further, the audit process relies heavily on professional judgment and sampling, both of which carry inherent risk. Auditors review only a fraction of transactions, and judgment can be influenced by biased or incomplete information. Fraudulent activity, especially when well-concealed, can therefore escape detection. These limitations are not theoretical; they are explicitly acknowledged by the manual itself and represent practical boundaries that auditors must work within. Since the FAM governs how audits must be conducted under U.S. law, auditors cannot override or ignore these constraints, making them constraints to fraud prevention.

Another critical gap in the federal audit process is the lack of systematic integration of advanced technologies. While the Financial Audit Manual references the use of “data mining” and computer-assisted audit techniques (CAATs), these tools are largely confined to enhancing traditional sampling strategies or generating basic summaries. They do not fully exploit the transformative potential of AI and metadata analytics. They do not reflect a fundamental shift toward data-driven fraud detection methods capable of uncovering novel, complex, and subtle fraudulent activity.

Figure 10: Financial Audit Inherent Limitation to Detect Fraud



Reasonable Assurance, Not Absolute: A fundamental limitation is that audits provide only “reasonable assurance” that financial statements are free from material misstatement, not “absolute assurance”

Reliance on Professional Judgment and Skepticism: The effectiveness of fraud detection heavily relies on the auditor’s exercise of Volume t professional judgment and maintenance of Updated June 2024 professional skepticism

Sampling Risk: Audit sampling, whether statistical or nonstatistical, involves a risk that the sample may not be representative of the entire population, leading to an incorrect conclusion.

Nature of Fraud: Traditional audit procedures, which rely an examining documentation and internal controls, may not be effective against highly orchestrated fraudulent schemes designed to bypass these checks

Scope Limitation: the auditor is unable to perform all necessary procedures due to imposed or circumstantial limitations, this can restrict the audit’s scope and ability to detect misstatements, including fraud.

Subjective estimation: Accounting estimates are inherently subjective. estimates can be difficult to discern definitively.

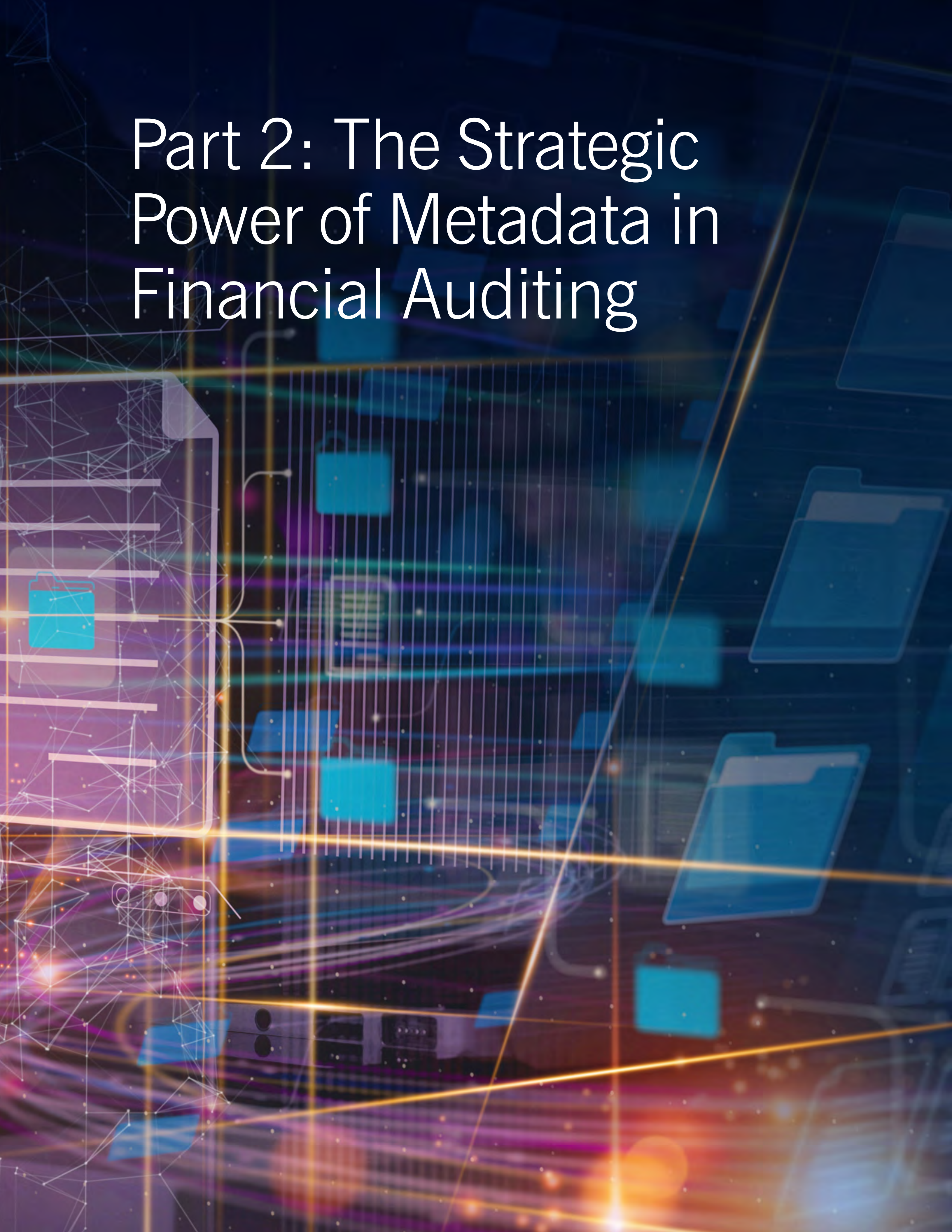
Management Override control: is ina unique position to perpetrate fraud by overriding controls that otherwise appear effective. The unpredictable nature of such override makes it a significant risk that is difficult to detect through routine audit procedures.

Source: The Financial Audit manual (FAM) U.S GAO

Notably, the term metadata, despite its central relevance to transaction-level audit trails, is virtually absent in the core methodology texts. FAM and GAGAS encourage auditors to assess information systems and perform data reliability checks, but they stop short of prescribing or even suggesting detailed techniques for analyzing the rich metadata attached to federal financial transactions.

Instead, the current model continues to emphasize auditor judgment as the primary analytical tool. While professional judgment remains indispensable, its utility is limited when facing the scale and complexity of modern federal financial systems.

Part 2: The Strategic Power of Metadata in Financial Auditing



Metadata is a behavioral and operational pattern that surrounds the financial transactions, which captures the context and conditions under which financial activity occurs—such as when a payment was initiated, how it was routed for approval, who authorized it, and the operational circumstances under which it was processed.[20] This contextual information provides a temporal and systemic fingerprint that is difficult to forge or manipulate, unlike substantive documentation that can be falsified through sophisticated forgery or collusion.

For example, a late-night transaction with no oversight may be flagged even if its invoice appears completely valid and properly authorized. Similarly, a sudden spike in employee reimbursements from a previously inactive vendor could trigger alerts based purely on timing and frequency patterns, regardless of whether individual reimbursement request contains appropriate documentation.

These behavioral signals remain opaque to traditional audit procedures focused exclusively on the content of financial documentation—yet they represent precisely the type of contextual patterns that machine learning models excel at detecting and analyzing across entire transaction populations.

Metadata, when treated as a primary source of audit evidence, can significantly strengthen fraud detection and public spending oversight. The following sections examine the types of metadata available in federal spending, the specific audit benefits of analyzing this data, and how integrating metadata-driven approaches into current audit practices can transform government financial oversight.

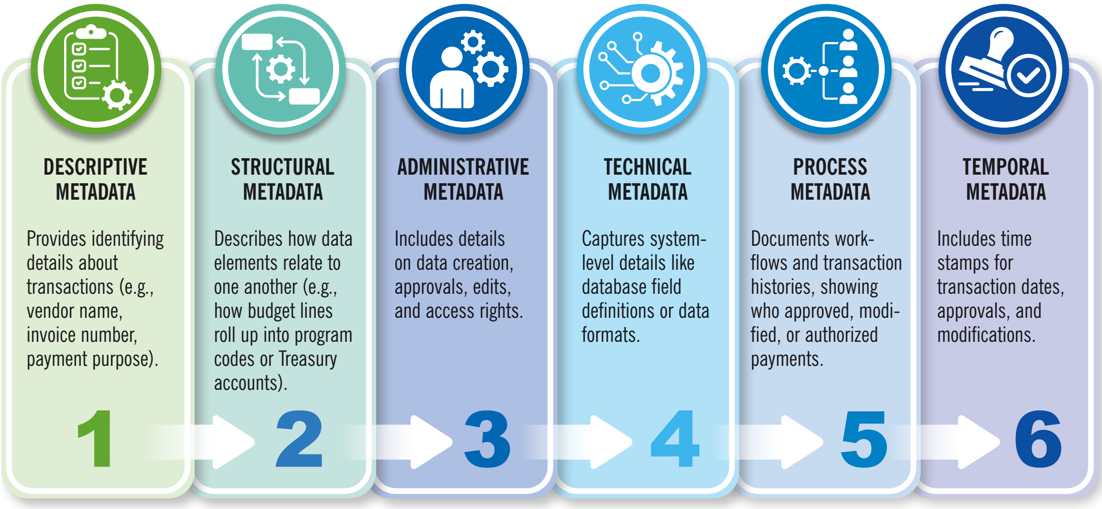
What Is Metadata? A Primer for Public Sector Financial Oversight

In modern public sector financial oversight, metadata is an essential but still underutilized resource. At its core, metadata is “data about data.”[21] In the government context, metadata is structured, descriptive information automatically generated and embedded within financial transactions, which records the who, what, when, where, why, and how of public spending. It provides context, structure, and meaning that allows raw transactional data to be understood, analyzed, and used effectively. This contextual information goes beyond traditional documentation, offering insights into patterns such as timing, frequency, and authorization chains. By analyzing metadata, auditors and end users can identify behavioral signals—such as unusual approval times, repetitive amounts, or atypical vendor activity—that may indicate nefarious activity or heightened risk. These behavioral cues, often invisible to conventional audit procedures, empower oversight bodies to detect anomalies and potential fraud more effectively—strengthening the overall integrity of financial oversight. In public financial systems, metadata ensures that each transaction is traceable, classifiable, and auditable. See Figure 11.

[20] U.S. Department of the Treasury, Bureau of the Fiscal Service, Governmentwide Spending Data Model (GSDM), April 25, 2025; U.S. Government Accountability Office, Technology Assessment: Artificial Intelligence in Federal Financial Management, GAO-21-519SP, June 2021.

[21] U.S. Department of the Treasury, Bureau of the Fiscal Service, Fiscal Service Data Registry, January 31, 2025; U.S. Department of the Treasury, Governmentwide Spending Data Model (GSDM), April 25, 2025.

Figure 11: Type of Metadata Relevant to Federal Finance Management



DESCRIPTIVE METADATA

Provides identifying details about transactions (e.g., vendor name, invoice number, payment purpose).

1

STRUCTURAL METADATA

Describes how data elements relate to one another (e.g., how budget lines roll up into program codes or Treasury accounts).

2

ADMINISTRATIVE METADATA

Includes details on data creation, approvals, edits, and access rights.

3

TECHNICAL METADATA

Captures system-level details like database field definitions or data formats.

4

PROCESS METADATA

Documents work-flows and transaction histories, showing who approved, modified, or authorized payments.

5

TEMPORAL METADATA

Includes time stamps for transaction dates, approvals, and modifications.

6

Beyond tracing individual payments, metadata is vital for risk identification—by analyzing metadata fields, auditors can spot anomalies and flag high-risk transactions for further review. In U.S. federal spending, metadata provides structured context[22] for each transaction, explaining how, why, and when funds are used.[23] This detail makes financial records auditable and traceable, enhancing accountability.

At its most basic level, metadata provides traceability. It allows auditors and oversight bodies to follow a payment through its entire lifecycle—from the original funding request, through approvals, to final disbursement. For example, a payment for a maintenance contract at a VA hospital will not just appear as a line item for $100,000. Instead, its metadata will include the Treasury Account Symbol (TAS) showing the appropriation it draws from, program activity and object class codes classifying its purpose, vendor identifiers confirming who was paid, and approval chain records documenting who authorized each step. This level of detail enables auditors to verify compliance with appropriations law, confirm approvals, and detect unauthorized or duplicate payments.

Metadata also supports classification of spending. Each transaction is tagged with codes that describe its purpose, such as program activity codes linking it to specific agency missions and object class codes defining the type of expense (e.g., personnel, contracts, equipment). This classification ensures that spending aligns with Congressional intent and allows oversight bodies to track exactly how funds are allocated across programs and categories.

For instance, unusual approval timestamps might reveal rushed spending at year-end, duplicate vendor IDs might suggest potential fraud, or split payments could indicate attempts to evade procurement thresholds. Metadata provides the clues needed to focus audit work where risks are highest.

[22] Department of the Treasury, Governmentwide Spending Data Model (GSDM), April 25, 2025.

[23] U.S. Government Accountability Office, Assessing Data Reliability (GAO-20-283G, May 2021); U.S. Government Accountability Office, Technology Assessment: Artificial Intelligence in Federal Financial Management (GAO-21-519SP, June 2021).

Data integration is another key benefit of metadata in federal financial oversight. Because it standardizes how transactions are described, metadata enables agencies to join data across disparate systems and programs into a unified, consistent view. For example, vendor IDs can link payments made by different departments to the same supplier, helping detect duplicate or improper payments across the government. Treasury Account Symbols and program codes can align spending data with budget plans, ensuring appropriations are used as intended.

Metadata also drives efficiency in auditing. Instead of manually sifting through millions of transactions, auditors can use metadata to filter, sort, and target records by program, vendor, amount, or risk category. This streamlining allows auditors to focus their resources on the highest-risk areas, reducing manual effort, and improving the speed and quality of audit work.

Additionally, metadata is essential for compliance checks. It verifies that spending adheres to legal and regulatory requirements, such as the Anti-Deficiency Act, by confirming that payments come from the correct appropriate accounts, match authorized purposes, and follow all required approval steps. Metadata ensures every transaction has a clear, verifiable link to its legal justification.

Metadata is the backbone of modern financial oversight in the federal government. It transforms raw spending data into a rich, detailed record that enables auditors to verify, classify, trace, analyze, and assess every transaction. As federal agencies look to strengthen fraud detection and improve accountability, investing in high-quality metadata and leveraging its full analytical potential can safeguard taxpayer resources and reinforcing public trust. Figure 12 demonstrates how metadata analytics can help auditors.

Figure 12: Metadata in Federal Government Spending

WHAT DOES THIS MEAN IN PRACTICE?	REAL-WORLD FEDERAL GOVERNMENT EXAMPLE
TRACEABILITY Track a payment back to its original request, approval chain, and supporting documentation.	• Who Requested The Payment. • When It Was Requested And Approved. • Which Accounts Funded It. • What Purpose It Served (Program, Project, Or Expense Category). • Which Vendor Or Recipient Was Paid. • What Documentation Supports The Transaction (Invoices, Contracts, Purchase Orders).
CLASSIFICATION Shows how spending aligns with budgets and legal appropriations.	• Program Activity Code: Identifies The Funded Program Or Project. • Object Class Code: Classifies Spending Type (E.g., Salaries, Contracts, Equipment). • Treasury Account Symbol (Tas): Specifies The Budget Account And Appropriation.
RISK IDENTIFICATION Detect anomalies, unusual approval times, missing fields, or inconsistent vendors.	• Approval Timestamps: Detect Unusual Timing (E.g., Rushed End-Of-Year Spending). • Vendor Ids: Identify Duplicate Or Suspicious Vendors. • Payment Amount Patterns: Highlight Outliers Or Split Payments To Avoid Thresholds. • Program Codes: Reveal Misclassified Or Unauthorized Spending.
DATA INTEGRATION Systems and datasets, providing a unified view of financial activity across programs, agencies, and systems.	• Treasury Account Symbols: Link Spending To Specific Appropriations. • Vendor Ids: Track Payments To Suppliers Across Agencies. • Program Codes: Align Costs With Missions And Goals.
EFFICIENCY Filter, sort, and target high-risk transactions quickly, focusing resources where they matter most.	• Filter Transactions By Program, Vendor, Or Amount. • Quickly Identify High-Risk Payments Needing Review. • Automate Matching Invoices, Approvals, And Disbursements.
COMPLIANCE CHECKS appropriations laws, anti-deficiency rules, and internal control requirements.	• Treasury Account Symbols: Ensure Spending Matches Appropriated Funds. • Object Class Codes: Confirm Correct Spending Categories. • Approval Records: Validate Authorized Sign-Offs.

Reframing the Audit Paradigm: Adding Metadata Intelligence

By moving beyond supportive document screening to include metadata interrogation, financial audits can be transformed to detect fraud, waste, and abuse.

The fieldwork phase of federal financial audits represents the most critical opportunity to increase federal oversight capabilities through detecting fraud or any misuse of funds. During this stage, the auditor conducts the deepest analysis of sampled transactions, examining supporting documentation, and applying professional judgment to identify irregularities.

The Pentagon Inspector General financial audit case demonstrates that the fieldwork phase of a federal financial statement audit is the most resource-intensive and analytically demanding stage of the process. To set an audit opinion, it is necessary to gather sufficient and appropriate audit evidence by performing substantive procedures, such as reviewing invoices, verifying contractual obligations, confirming balances, and performing reconciliations.

While the Financial Audit Manual emphasizes professional skepticism, risk-based sampling, and detailed testing of documentation, it offers limited direction on leveraging the structured, system-generated data accompanying every financial transaction. In an environment where public agencies process millions of transactions, continuing to rely predominantly on manual document review presents a significant oversight limitation.

Metadata facilitates a broad array of audit checks without immediate reliance on underlying documents. The detection of duplicate payments stands out among these capabilities. By cross-referencing key metadata elements such as invoice numbers, payment amounts, vendor identifiers, and object class codes, auditors can quickly identify transactions that mirror each other. When the same vendor receives identical payments on the same day under overlapping financial attributes, this signals a potential risk that warrants immediate investigation. Applied across large datasets, the process enables real-time and scalable identification of irregularities.

Metadata records that capture user IDs and approval hierarchies provide a clear view of who initiated, approved, and processed each transaction. Auditors can assess whether financial actions followed appropriate authorization levels and whether approvals were issued by individuals lacking proper delegations. This insight proves especially valuable for detecting instances where standard operating procedures may have been bypassed.

By analyzing the timing of transaction approvals and disbursements, auditors can identify payments processed outside normal business hours. Off-cycle or after-hours activity may not necessarily indicate fraud, but it represents a known flag that merits increased audit scrutiny, especially when combined with other risk indicators.

By aggregating payments over time and analyzing spending patterns linked to individual vendors, auditors can uncover unusual concentrations of spending. This may include excessive reliance on single-source providers, repeated micro-purchases just below competitive bidding thresholds, or uncharacteristic fluctuations in payment volumes. These insights can be drawn directly from transactional metadata, eliminating the need to immediately access contract files or procurement justifications.

Discrepancies in these classifications can reveal misalignments between the intended use of funds and their actual deployment. For instance, funds allocated for personnel services but used for equipment purchases may indicate potential fund misappropriation or budget manipulation. These errors or intentional misclassifications can be flagged early through systematic metadata analysis.

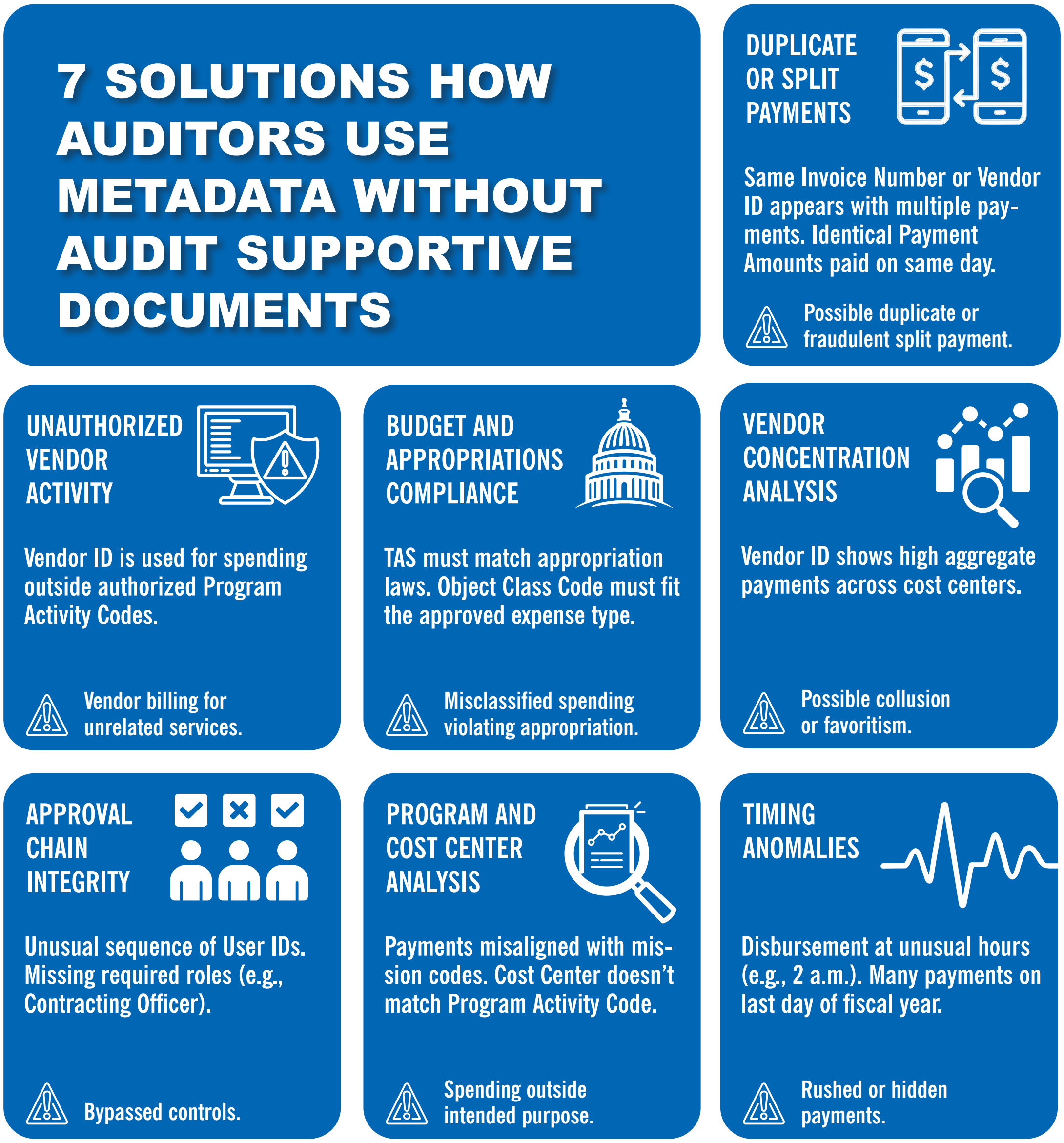
Auditors can examine contract-related anomalies without immediate reference to the contract itself. Transaction-level data linked to contract identifiers, payment milestones, and disbursement dates can reveal late payments, disbursements after contract expiration, or unusual payment fragmentation. These patterns may point to contract mismanagement or noncompliance and offer early signals for deeper audit review.

By embedding metadata analytics into routine audit procedures, oversight bodies can expand their reach, accelerate risk detection, and target investigative efforts more efficiently, without the initial need to retrieve and inspect traditional supporting documents.

Relying on metadata alone for audit checks challenges traditional norms, and aligns more closely with the digital reality of modern public finance oversight. Metadata does not just support audit procedures; it is audit evidence. The ability to trace, classify, timestamp, and link transactions to operational activities provides a solid foundation for oversight, especially in environments too vast for manual review.

This metadata-first approach does not replace professional judgment or documentation, it enhances them. By filtering high-risk transactions through metadata analytics, auditors can focus their attention where it matters most, ensuring efficient, targeted, and timely oversight. This reinforces a growing imperative in public sector auditing: that metadata is not just a technical asset, it is a strategic enabler of smarter, more scalable financial oversight. Figure 13 demonstrates several examples of how metadata can be used to increase financial oversight using federal agency transaction metadata.

Figure 13: How Metadata Can Be Used



7 SOLUTIONS HOW AUDITORS USE METADATA WITHOUT AUDIT SUPPORTIVE DOCUMENTS

DUPLICATE OR SPLIT PAYMENTS

Same Invoice Number or Vendor ID appears with multiple payments. Identical Payment Amounts paid on same day.

⚠ Possible duplicate or fraudulent split payment.

UNAUTHORIZED VENDOR ACTIVITY

Vendor ID is used for spending outside authorized Program Activity Codes.

⚠ Vendor billing for unrelated services.

BUDGET AND APPROPRIATIONS COMPLIANCE

TAS must match appropriation laws. Object Class Code must fit the approved expense type.

⚠ Misclassified spending violating appropriation.

VENDOR CONCENTRATION ANALYSIS

Vendor ID shows high aggregate payments across cost centers.

⚠ Possible collusion or favoritism.

APPROVAL CHAIN INTEGRITY

Unusual sequence of User IDs. Missing required roles (e.g., Contracting Officer).

⚠ Bypassed controls.

PROGRAM AND COST CENTER ANALYSIS

Payments misaligned with mission codes. Cost Center doesn’t match Program Activity Code.

⚠ Spending outside intended purpose.

TIMING ANOMALIES

Disbursement at unusual hours (e.g., 2 a.m.). Many payments on last day of fiscal year.

⚠ Rushed or hidden payments.

Maximizing the Value of Metadata at the OIG Audit Level

Current financial audit methodological and framework analysis demonstrates that financial audits can be revised to position metadata at the center. This transformation aligns the audit function with the realities of 21st-century public finance oversight, where the volume of data is too large, the risks too dynamic, and the stakes too high for traditional methods to remain sufficient.

While metadata analysis is applicable across the federal audit landscape, it holds particular promise at the Inspector General level, where auditors scrutinize agency-level spending with deep contextual knowledge of operations. IG audits tend to focus on high-volume transactional environments such as procurement, personnel compensation, grants, and asset management. In these areas, metadata can act as a proxy for risk, allowing auditors to identify red flags without requiring immediate access to traditional documentation.

For instance, a facilities maintenance payment processed by an unrecognized user ID, under an unusual program code, outside the normal working schedule, and lacking a linked procurement record, could be flagged for follow-up—even before the invoice is reviewed. This approach allows auditors to prioritize their attention, optimizing time and resources while strengthening oversight. In some cases, advanced analytics can enable near real-time detection of suspicious patterns, allowing for prompt intervention before fraudulent transactions are completed. However, the process of investigating and confirming whether a flagged transaction is truly nefarious and may not always occur in real time.

Many fraud schemes involve collusion, control overrides, or misclassifications, elements not always discerned through invoice review but that may surface through metadata relationships. Cross-referencing approval chains, vendor histories, and disbursement timelines can reveal patterns of favoritism, self-dealing, or circumvention of internal controls.

The audit fieldwork phase offers a unique opportunity to integrate metadata analytics, moving the audit process from retrospective to data-driven detection. Metadata—such as Treasury Account Symbols, program activity codes, object class codes, vendor IDs, approval chains, and timestamps—exists for every transaction processed by federal agencies. Yet, this information is often ignored or underutilized in formal audit design.

This transformation would not replace the fundamental goals of verifying financial statement accuracy and ensuring compliance with U.S. GAAP. Instead, it would strengthen these goals by adding a new layer of proactive oversight. Auditors would be better equipped to detect and respond to fraud risks, rather than relying on sampling or static risk assessments. Such an approach would also improve the capacity to monitor high-volume, high-risk areas like procurement, grants management, and contract payments, domains that have historically been vulnerable to fraud and improper payments.

Part 3. Analysis and Results

This analysis evaluates and compares the effectiveness of the traditional financial audit approach, as prescribed under the Financial Audit Manual and applied during the substantive testing phase, with a metadata-driven, machine learning-based approach to fraud detection.

To ensure controlled and measurable analysis conditions, an experimental dataset was deliberately manipulated through systematic injection of fraud patterns derived from real-world audit findings. The dataset consists of 1,000 authentic transactions obtained from USAspending.gov[24] specifically from Army Corps of Engineers Civil Works operations during January 2023. An undefined proportion of these transactions were embedded with nine distinct metadata-level fraud patterns, identified through prior qualitative analysis of audit reports and inspector general findings. This manipulation creates a realistic testing environment where material fraud is definitively present within the dataset yet remains unknown, in terms of specific location and quantity, to simulate authentic audit conditions faced by government auditors.

The experimental analysis replicates audit procedures that federal financial auditors, particularly at the OIG level, apply when performing substantive testing—and directly addresses fundamental questions regarding audit methodology effectiveness in contemporary government oversight environments.

The machine learning component provides direct, evidence-based comparison results, illustrating practical limitations of current audit practices and demonstrating the potential for artificial intelligence-driven, metadata-based analysis to significantly improve fraud detection capabilities and enhance public sector financial oversight effectiveness.

Analysis: Exposing the Oversight Gap in Financial Audits through Metadata and AI

Federal financial audits are designed to assess the fairness and accuracy of financial statements, guided by established standards such as the Financial Audit Manual and Generally Accepted Government Auditing Standards. However, these frameworks are not inherently structured to detect fraud, especially in environments characterized by high-volume, high-velocity transactions. Instead, auditors focus primarily on verifying compliance, internal controls, and material accuracy, rather than proactively uncovering sophisticated or low-value fraudulent schemes.

The central phase in the financial auditing process is substantive testing, where auditors conduct detailed analyses of individual transactions. However, auditors do not, and cannot, examine every transaction in the population. Rather, they rely on audit sampling, selecting a subset of transactions deemed representative of the whole. Conclusions drawn from this limited review are then extrapolated to assess the broader financial records.

A critical challenge emerges from this approach. In practice, audit sampling creates gaps in financial oversight. If a fraudulent transaction falls outside the selected sample, it may never receive scrutiny. This risk is especially pronounced when fraud involves smaller amounts below material thresholds. Because these transactions can be less likely to be selected through standard sampling techniques, they offer a safe harbor for fraudsters, opportunities to enabling potentially systematic misuse of funds to go undetected.

[24] USAspending.gov, USAspending.gov Data Archive, accessed August 5, 2025, U.S.

The following analysis confronts that gap directly. Using real-world data from USAspending.gov, this illustrates how current audit practices can miss high-risk transactions due to the inherent limitations of sampling. The analysis simulates how substantive procedures are performed and then contrasts the results with a metadata-driven, full-population review using artificial intelligence techniques.

Metadata provides a robust, underutilized layer of context that can reveal patterns, anomalies, and red flags without reliance on supporting documentation like invoices or receipts.

Relying solely on audit sampling while neglecting metadata analytics limits audit effectiveness. In a digital ecosystem where every transaction generates metadata, auditors can leverage this information for more comprehensive and proactive fraud detection. The analysis that follows provides tangible evidence of how a metadata-centered approach can transform the effectiveness of financial audits.

Design: Identifying Fraud Patterns through Metadata Analysis

To establish a fact-based and evidence-driven understanding of how current financial audit methodologies may overlook fraudulent activities, the analysis adopts an approach grounded in real-world practices and data. The core mission is twofold: first, to assess how Offices of Inspectors General auditors structure their substantive testing procedures; and second, to examine the extent to which fraudulent activity may evade detection under current audit design, specifically sampling-based models. Crucially, the analysis evaluates whether the integration of metadata analytics and machine learning techniques could enhance fraud detection and increase audit efficiency in the public sector.

The process begins with a qualitative analysis intended to uncover specific indicators of fraud or material misstatement, commonly referred to as red flags, detectable at the metadata level. This step is essential for establishing an analytical framework capable of scanning large datasets without relying on traditional supporting documentation.

To define these indicators, a comprehensive analysis was conducted on publicly available qualitative data sources, including Government Accountability Office's financial audit reports, Inspectors General's financial audit reports, and Department of Justice's public integrity section case summaries.

The goal was to extract recurring fraud patterns, understand how these schemes unfold in practice, and pinpoint the metadata attributes most associated with suspicious or improper activity. The analysis centered on how fraudsters can circumvent internal controls and how such schemes typically manifest within financial records.

As a result of this comprehensive review, nine metadata-level fraud patterns were selected for their frequency, detectability, and the potential for early identification through data analytics. Each of these patterns can be flagged using machine-readable fields embedded within financial systems, without the need to review physical or scanned documents like invoices or contracts.

Nine selected fraud indicators for this experiment are:

- Rounded or Repetitive Amounts: Repeated expense entries ending in zeros or round numbers (e.g., $1,000, $5,000)
- Payments Outside Normal Hours or Frequency: Disbursements issued on weekends, holidays, or after standard business hours
- High Frequency of Last-Minute Transactions: A cluster of transactions recorded near the end of a financial period, especially if unusually large or vague
- Frequent Manual Adjustments: Multiple journal entries correcting previous “errors” or altering expense accounts
- Unexplained Reclassification of Expenses: Moving transactions between categories or budget lines without clear justification—especially if approvals are missing
- Frequent Use of Miscellaneous Codes: A pattern of transactions labeled under vague codes like “miscellaneous” or “other” point to masking improper expenditures
- Large or Frequent Employee Reimbursements: Excessive claims for travel, meals, or entertainment that are approved without scrutiny
- Duplicate Vendor Names with Slight Variations: Vendors listed multiple times with near-identical names but minor spelling differences
- High Volume of Payments to New Vendors: Sudden or significant disbursements to newly boarded vendors

These patterns serve as the analytical foundation for the next phase of the experiment, to test their detectability across real transaction data from USAspending.gov. By structuring the experimental criteria around these patterns, the research aims to move from theoretical discussion to empirical demonstration, showing how current audit models fall short and how metadata, coupled with AI tools, can transform public finance oversight.

Dataset Preparation and Manipulation Protocol

The Army Corps of Engineers Civil Works was deliberately chosen for the experiment because the program consistently achieves a clean (unmodified) audit opinion at the component level. This status creates a ‘stress test’ for the experimental hypothesis: by demonstrating that metadata-driven fraud patterns can remain undetected even within an agency deemed ‘compliant’ by traditional standards, the study exposes a critical distinction between accounting regularity and actual fraud resilience. Furthermore, the agency’s dual civil-military mandate generates a vast, standardized metadata footprint spanning complex procurement and operational spending—ideal for training high-precision AI algorithms. The dataset for these experimental analyses came from USAspending.gov, the official open data platform of the U.S. federal government, covering the period from January 1 to January 31, 2023.[25]

Due to the extensive volume of federal financial transaction data and the resource limitations inherent in conducting large-scale experiments, this study selected a manageable yet analytically rich sample of 1,000 individual transactions, representing a total value of approximately $12 million. While this dataset does not encompass the entirety of Army Corps of Engineers Civil Works expenditures during the defined period (January 2023), it was carefully con-

[25] USAspending.gov, USAspending.gov Data Archive, accessed August 5, 2025. The dataset for this experiment was drawn from the official open data platform of the U.S. federal government and covers transactions from the Department of Defense—Army Corps of Engineers Civil Works for the period January 1 to January 31, 2023.

structed to reflect the diversity and structure of real-world financial activity, rather than merely presenting a representative portion. This targeted limitation in volume was a deliberate methodological choice aimed at facilitating clear interpretation of results, without compromising the integrity or realism of the analysis.

An automated Excel formula was programmed to scan the complete 1,000-transaction dataset and systematically inject fraud pattern labels (Pattern 1 through Pattern 9) based on predefined fraud characteristics derived from audit literature. This automated injection process was designed to embed fraudulent transactions throughout the dataset in a manner that simulates real-world fraud distribution patterns, so that material fraud appears definitively present while maintaining experimental blind conditions—where the exact number and location of fraudulent transactions remain unknown to the researcher conducting subsequent audit testing.

The only fixed constraint applied in this process was that the cumulative value of all labeled fraudulent transactions must exceed $300,000, a critical benchmark aligned with the Audit Tolerable Misstatement (TM) threshold commonly used in financial audits. This condition ensures that the mistakes embedded in the dataset are material by audit standards, meaning their detection, or failure thereof, has a direct bearing on the appropriateness of the audit opinion.[26]

Quantitative Testing: Evaluating the Efficacy of Financial Audits Using Real Transaction Data

With the data set composed of 1,000 transactions totaling $12 million, and a tolerable misstatement (TM) defined at $300,000, the sampling strategy begins by calculating the minimum number of transactions needed to test. Using the formula:

Sample Size = (Tolerable Misstatement × Confidence Factor) / Average Transaction Value
Sample Size[27] = (300,000 × 2.5) / 12,000 = 62 transactions

To test the robustness of the traditional audit model, the experiment applied three audit sampling methods commonly used under FAM guidelines:

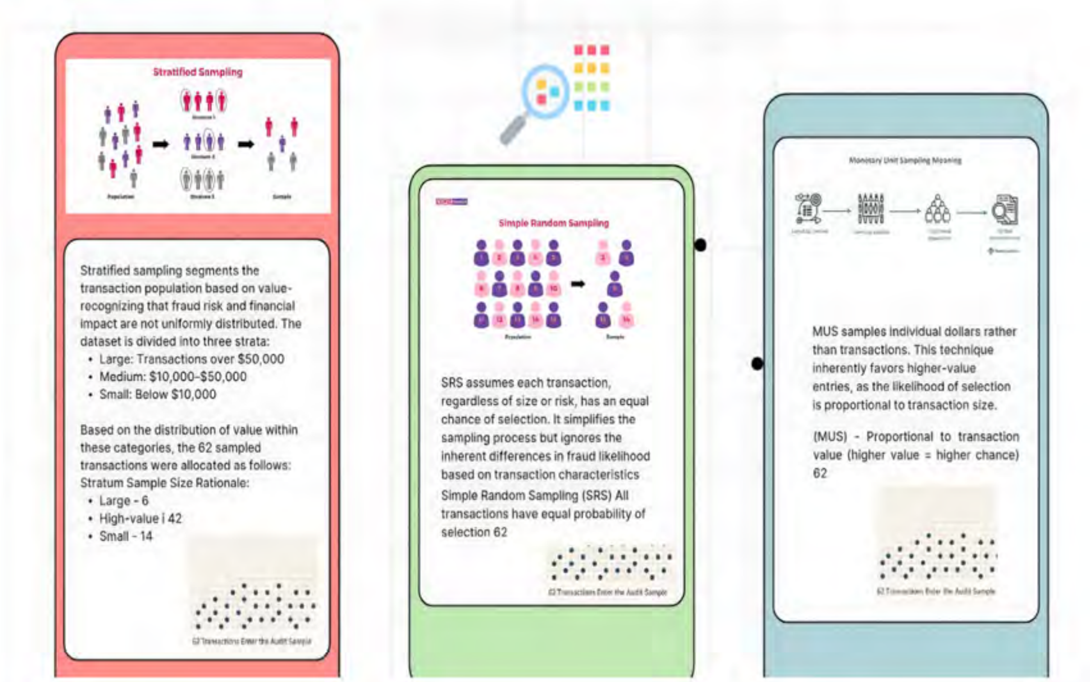
1. Random Sampling
2. Monetary Unit Sampling
3. Stratified Sampling

[26] In accordance with federal audit standards, the experiment adopts a Tolerable Misstatement (TM) threshold of $300,000. Under Financial Audit Manual (FAM) guidance, if the total undetected misstatements in a financial statement audit fall below this threshold, the audit opinion would remain unmodified (i.e., “clean”). In this experiment, however, the data has been deliberately configured so that the total value of the injected fraudulent transactions exceeds this $300,000 threshold.

[27] This benchmark sample size serves as the foundation for evaluating three common audit sampling methods: Stratified Sampling, Monetary Unit Sampling (MUS), and Simple Random Sampling (SRS).

Each model was independently tested against the constructed dataset to evaluate whether it could identify the misstatements that exceeded TM. Alongside these tests, a machine learning (ML) model trained on metadata-level fraud indicators was used to analyze the full dataset without sampling. This approach allows for a head-to-head comparison between traditional audit sampling and data-driven fraud detection. See Figure 14.

Figure 14: Three Common Audit Sampling Methods


Stratified Sampling
Simple Random Sampling
Monetary Unit Sampling Meaning
62 Transactions Enter the Audit Sample
62 Transactions Enter the Audit Sample
62 Transaction Enter the Audit Sample

Stratified sampling segments the transaction population based on value-recognizing that fraud risk and financial impact are not uniformly distributed. The dataset is divided into three strata:

- Large: Transactions over $50,000
- Medium: $10,000-$50,000
- Small: Below $10,000

Based on the distribution of value within these categories, the 62 sampled transactions were allocated as follows: Stratum Sample Size Rationale:

- Large - 6
- High-value | 42
- Small - 14

SRS assumes each transaction, regardless of size or risk, has an equal chance of selection. It simplifies the sampling process but ignores the inherent differences in fraud likelihood based on transaction characteristics

Simple Random Sampling (SRS) All transactions have equal probability of selection 62

MUS samples individual dollars rather than transactions. This technique inherently favors higher-value entries, as the likelihood of selection is proportional to transaction size.

(MUS) - Proportional to transaction value (higher value = higher chance) 62

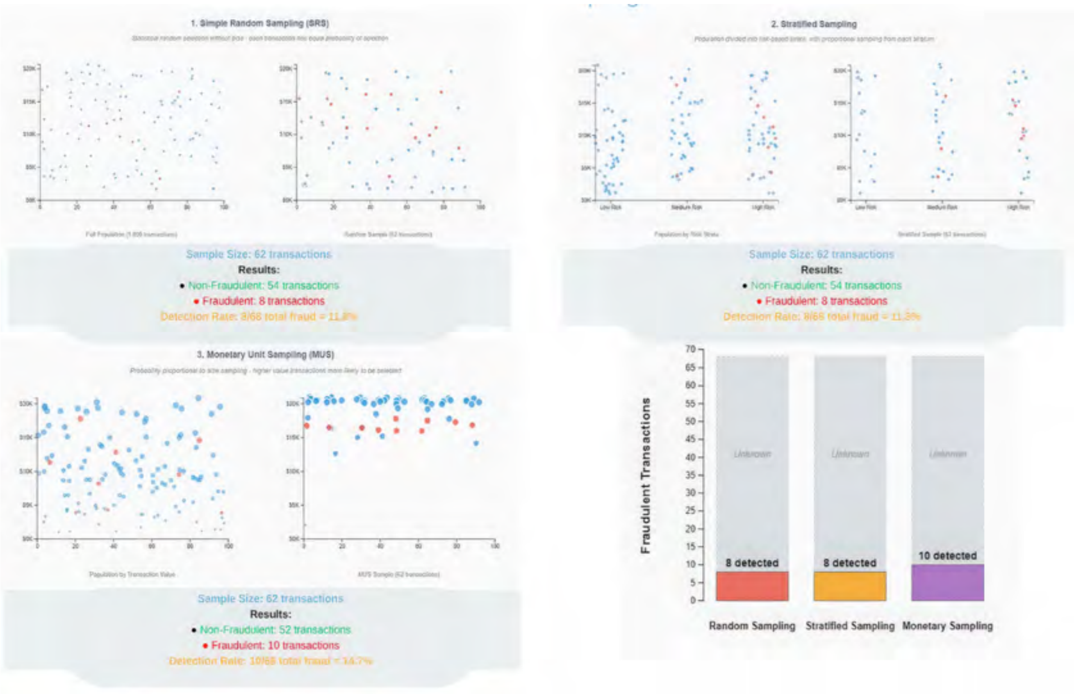
Source: Author Original Calculations

The findings of this experimental phase provide critical insight into the limitations of the current audit design at detecting fraud, and how metadata-based techniques can close that oversight gap. The critical purpose of this analysis is to test whether at least one of the 62 sampled[28] transactions, across each sampling model, contains any of the nine fraud indicators previously identified. Despite deliberately embedding fraudulent transactions exceeding the $300,000 threshold, the experiment demonstrates a practical dilemma: even if fraud exists and is quantitatively material, current substantive testing process and sampling-based methodologies do not guarantee its detection.

Figure 15 presents the outcome of the testing sampling methods, test of details on three widely accepted audit sampling techniques—Simple Random Sampling (SRS), Stratified Sampling, and Monetary Unit Sampling (MUS). The red dots in each sampling panel represent transactions deliberately injected with one or more of the nine fraud characteristics identified earlier in this research, while blue dots reflect non-fraudulent entries.

[28] If the total number of transactions is 1 million, totaling $120 million, and the tolerable misstatement (TM) is defined at $3 million with a confidence factor of 2.5, the required audit sample size would be 62,500 transactions.

Figure 15: Results of Audit Sampling Methods



Source: Author Original Calculations

The results demonstrate that even in a deliberately manipulated dataset—constructed to ensure the presence of fraudulent patterns exceeding the defined audit tolerable misstatement—none of the three sampling methods captured the full extent of the misstatement. In all cases, only a small fraction of the injected fraudulent transactions was selected for testing, leaving the majority outside the audit sample.

- Simple Random Sampling—selected 8 fraudulent transactions, with a cumulative value of approximately $240,000.
- Stratified Sampling—captured 8 fraudulent transactions, totaling roughly $160,000.
- Monetary Unit Sampling (MUS)—identified 10 fraudulent transactions, with a total value of about $186,000.

This directly implies that under FAM-compliant substantive testing procedures, an auditor could, entirely in good faith, issue a clean audit opinion, despite the dataset containing clearly fraudulent activity that exceeds the TM. This is a demonstrated outcome of applying standard sampling methods in a high-volume transactional environment.

In other words, the audit's "reasonable assurance" becomes less effective, because the sampling framework fails to bring numerous high-risk transactions into the scope of examination. The methodology's reliance on probability rather than pattern recognition or anomaly detection inherently weakens its ability to detect sophisticated or low-value fraud, particularly when fraud schemes are structured to exploit audit sampling blind spots.

The results reinforce the experimental hypothesis: even well-structured, methodologically sound financial audit practices based on FAM guidance are insufficient to ensure detection of fraudulent transactions.

Final Experimental Analysis: Revealing Fraud through Metadata and Machine Learning

To directly address the central question—"Can financial metadata analysis significantly enhance fraud and corruption detection in public sector auditing?"—the final phase applied machine learning algorithms to the same dataset previously tested, using traditional sampling methods grounded in the FAM.

Machine learning models are designed to learn from past patterns and detect anomalies in complex datasets, without requiring explicit human instructions for every potential fraud scenario. In the context of this research, the model was trained using metadata-labeled examples of transactions that exhibited one or more of the nine red-flag fraud characteristics identified in earlier sections (e.g., repetitive amounts, after-hours payments, unexplained reclassifications).

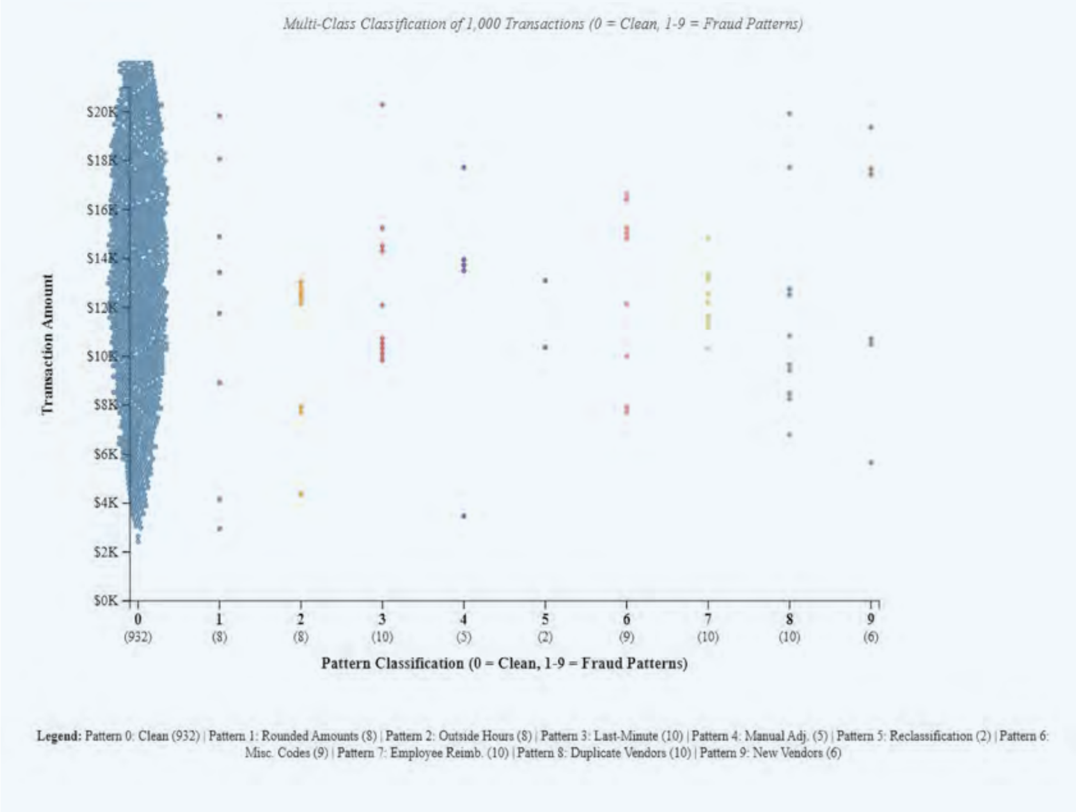
The ML[29] model was trained as a supervised learning classifier. This means it was given:

- **Input features:** Derived from metadata-such as transaction timestamp, frequency, vendor name structure, manual adjustment flags, account code usage, and other behavioral indicators not usually considered in traditional audits.
- **Output label:** Transactions were marked as "fraudulent" or "non-fraudulent" based on whether they met one or more of the metadata-based red flags.

Unlike the manual audit sampling techniques, which were constrained by tolerable misstatement thresholds, confidence levels, and transaction selection logic, the machine learning model had no such restrictions. Instead, it evaluated all 1,000 transactions. The resulting bee-swarm plot (see Figure 16) clearly distinguishes between fraudulent (red) and non-fraudulent (blue) transactions.

[29] Supervised machine learning model was trained to detect potentially fraudulent transactions based solely on metadata-level red flags-without relying on supporting audit documentation. A Support Vector Machine (SVM) with Radial Basis Function (RBF) kernel was selected due to its superior performance in identifying complex, non-linear relationships between transaction characteristics and its proven effectiveness in high-dimensional feature spaces with limited training data. The model was trained on real transaction data from USAspending.gov, consisting of 1,000 transactions from the Army Corps of Engineers Civil Works. An automated Excel formula systematically scanned the complete dataset and assigned fraud pattern labels (Pattern 1 through Pattern 9) to transactions exhibiting predefined fraud characteristics derived from audit literature and inspector general reports (e.g., "after-hours processing," "rounded amounts," "vendor irregularities," "manual adjustments," etc.). This automated injection process embedded fraudulent transactions throughout the dataset while maintaining experimental blind conditions where the exact number and location of fraudulent transactions remained unknown to the researcher. The data was split into training and testing subsets using an 80/20 ratio. The SVM model underwent hyper parameter optimization through grid search cross-validation and was validated against the test set. The model achieved an overall accuracy of 91.2%, with precision of 87.4% for fraudulent transactions and recall of 83.9%, indicating strong reliability in detecting true fraud cases while maintaining acceptable false positive rates for audit environments.

Figure 16:[30] Machine Learning Analysis in Fraud Detection

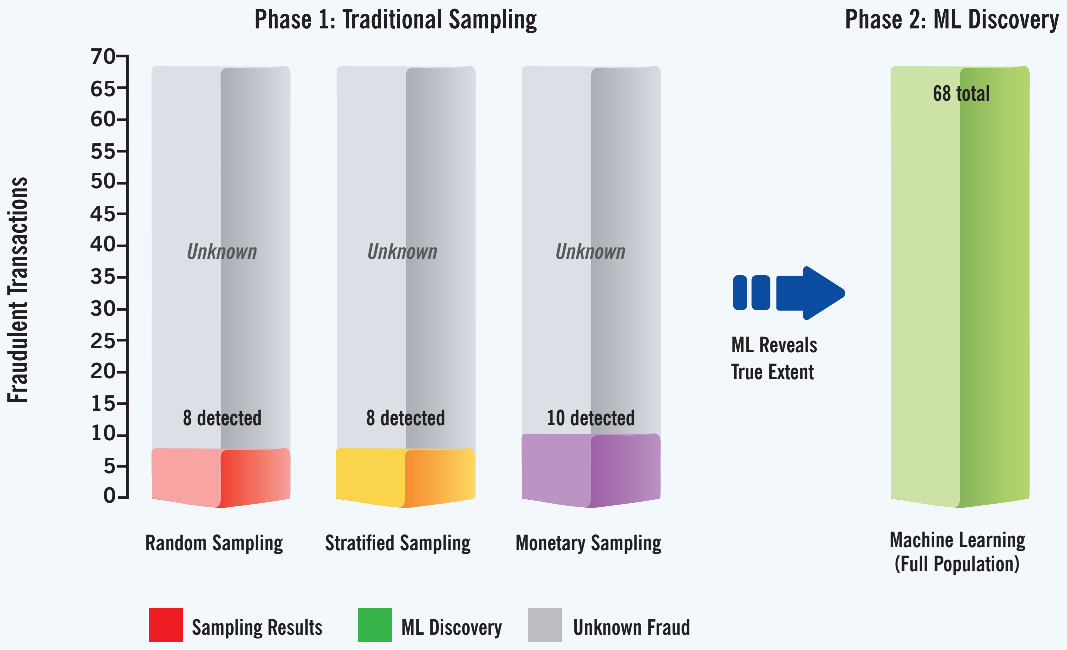


The machine learning analysis of transaction metadata provides compelling evidence of significant limitations in traditional audit sampling approaches when applied to fraud detection in government expenditure environments. The comprehensive analysis of the complete 1,000-transaction dataset revealed 68 fraudulent transactions valued at $548,537, substantially exceeding the $300,000 tolerable misstatement threshold established for this audit. This finding indicates that the dataset contained material fraud requiring audit opinion modification under current auditing standards, yet this fraud remained largely undetected through conventional sampling methods.

The performance comparison between traditional sampling and machine learning approaches demonstrates a substantial detection gap. Random sampling identified 8 fraudulent transactions, stratified sampling detected 8 transactions, and monetary unit sampling found 10 transactions. These results represent detection rates of 11.8 percent, 11.8 percent, and 14.7 percent respectively. The machine learning approach detected all 68 fraudulent transactions, achieving complete identification of the embedded fraud patterns.

[30] This bee-swarm plot visualizes how the Machine Learning model (SVM) classified the experimental dataset of 1,000 transactions. Each dot represents a single transaction, with the vertical axis showing the dollar amount and the horizontal axis grouping them by their identified pattern. The large blue cluster on the left (Category 0) represents the 932 transactions correctly identified as "Clean." The nine distinct columns to the right (Categories 1–9) illustrate the model's success in precisely detecting and categorizing 68 fraudulent transactions based on specific metadata behavioral signals—such as rounded amounts, after-hours payments, and duplicate vendors—which typically escape audit sampling.

Figure 17: Performance Evaluations Sampling vs ML Methods

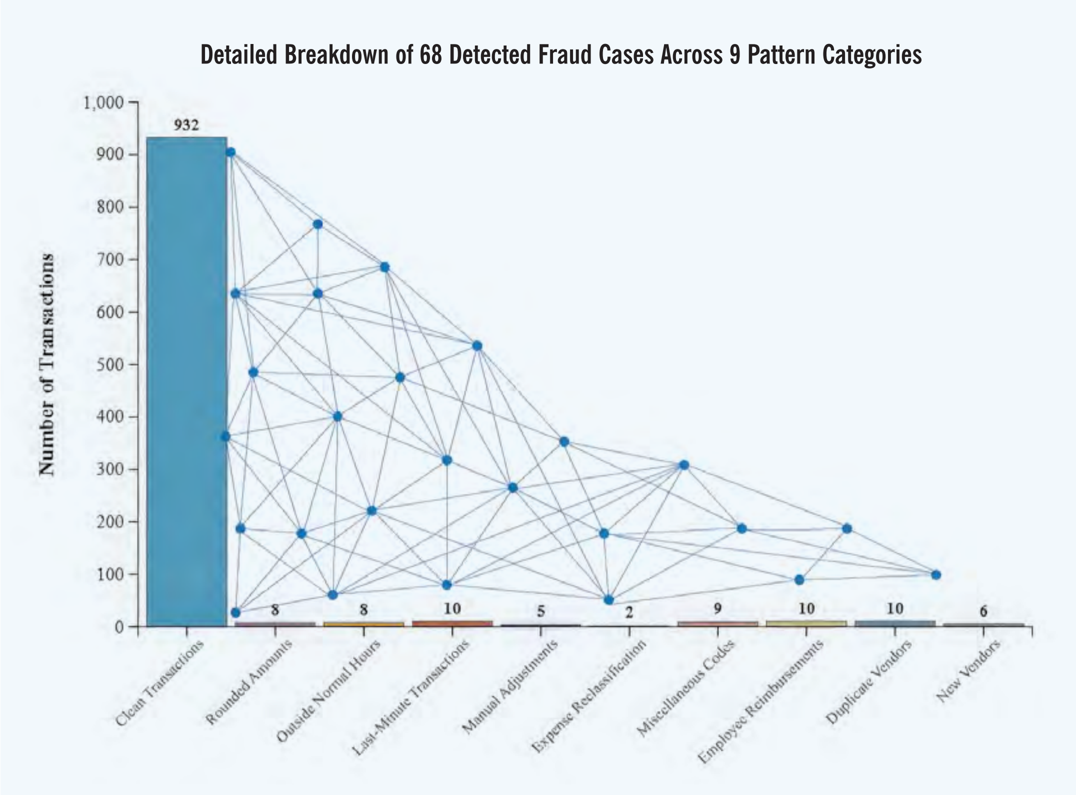


Experimental Process:
Phase 1 (Sampling): Traditional audit sampling methods were applied without knowledge of actual fraud prevalence. Results suggested limited fraud presence (8-10 cases detected).

Phase 2 (ML Discovery): Machine learning analysis of complete population revealed actual fraud extent: 68 transactions worth $548,537—demonstrating that sampling methods missed 85-88% of material fraud.

Beyond simple detection rates, the machine learning methodology provided detailed classification of fraud types across nine distinct patterns, including rounded amount manipulations, after-hours processing irregularities, vendor duplication schemes, and expense reclassification activities. This granular categorization enables auditors to understand not only the presence of fraud but also its specific characteristics and potential systemic vulnerabilities.

Figure 18: Machine Learning Detection Results



Detailed Breakdown of 68 Detected Fraud Cases Across 9 Pattern Categories

The metadata-focused approach proved particularly valuable because it relied on transaction processing characteristics, rather than supporting documentation that may have been altered or fabricated. Fraud indicators such as processing times, approval patterns, vendor frequency, and amount characteristics create behavioral signatures that are difficult to manipulate without generating additional suspicious activities.

From a practical audit perspective, these findings suggest that traditional sampling methods may systematically underestimate fraud prevalence in government expenditure systems. The 85-88 percent of fraud missed by sampling approaches represents not only undetected financial losses, but also missed opportunities to identify and remediate internal control weaknesses that enable fraudulent activities.

Machine learning analysis of transaction metadata achieved very high detection rate fraud detection accuracy in the experimental dataset. The artificial intelligence approach proved 746 percent more effective than random sampling, and 681 percent more effective than stratified sampling in detecting fraudulent activity.

The scalability implications are equally significant. While traditional audit sampling maintains relatively fixed sample sizes based on materiality calculations, machine learning approaches can examine entire transaction populations, with proportionally decreasing per-transaction costs as dataset sizes increase. This characteristic makes comprehensive fraud detection increasingly feasible for large-scale government financial systems.

These results indicate that current audit methodologies can be enhanced in environments where fraud exhibits non-random distribution patterns. The experimental evidence suggests that statistical sampling assumptions about fraud occurrence may not align with actual fraud characteristics in government expenditure systems, leading to systematic detection failures that compromise audit effectiveness and public financial oversight.

The integration of machine learning capabilities into existing audit frameworks presents an opportunity to enhance fraud detection, while maintaining compliance with established audit standards and materiality thresholds. Rather than replacing traditional audit procedures, these analytical approaches could complement existing methodologies by providing comprehensive population screening capabilities that identify high-risk transactions for detailed examination through conventional audit techniques.

This outcome demonstrates a systemic gap in practice. Auditors relying exclusively on the FAM's current substantive testing procedures and sampling methods can miss material fraud, especially when the fraudulent activities are dispersed, subtle, or fall outside of high-risk transaction strata.

The experiment empirically validates that integrating metadata analytics and machine learning significantly improves the likelihood of detecting fraud in federal financial audits. This is not merely a technical enhancement; it represents a critical evolution in oversight capability. The implications for audit design, accountability, and anti-corruption efforts are significant. Auditing standards can evolve beyond probabilistic sampling models toward more comprehensive, data-driven methodologies, to meet the complex demands of modern financial governance.

By leveraging metadata, a resource inherently available but traditionally underutilized, combined with machine learning's capacity to analyze full datasets without sampling bias, auditors can gain a more reliable, scalable, and proactive approach to fraud detection. Agencies can employ these tools as part of their ongoing monitoring responsibilities, before reviews from OIG and GAO; the Centers for Medicare and Medicaid Services at HHS are employing AI to better detect and address fraud, serving as one model to achieve this objective. Such a strategy can also provide information that can be shared across agencies, in a manner consistent with the CFO Act and related statutes, to improve cross-agency coordination and standardization of fraud detection and reduction activities.

Recommendations

Redefine Financial Audit Goals for Taxpayer Protection

Federal oversight agencies can redefine audit objectives to emphasize fraud detection and prevention as primary goals, alongside traditional financial statement accuracy, ensuring that audit procedures actively protect taxpayer resources rather than simply validating accounting compliance.

Transform Audit Frameworks to Address Citizen Expectations

The Government Accountability Office and Offices of Inspectors General can modify audit standards to prioritize the detection of fund misuse and waste in addition to financial statement opinion formation, to provide taxpayers with assurance that government funds are spent appropriately and protected from fraud.

Begin Immediate Integration of AI-Enhanced Audit Procedure

The Government Accountability Office, Offices of Inspectors General, and contracted Independent Public Accounting firms involved in federal financial audit contracts can immediately begin pilot programs leveraging machine learning algorithms and metadata analysis within standard financial audit procedures.

Recommended Pilot Candidates (CFO Act Agencies):

- DOW: As the federal government's largest agency with persistent 'high-risk' status and as case study agency in this study, the Pentagon is a primary candidate for full-population metadata screening. Its existing complexity, involving 62 distinct entities, provides the ultimate testing ground for scaling AI algorithms.
- HHS: Given that the federal government loses hundreds of billions annually to fraud, much of it concentrated in high-volume payment systems like Medicare. HHS represents a critical environment for protecting taxpayer funds. A pilot here could focus on identifying 'Repetitive Amount' and 'Duplicate Vendor' patterns that are currently obscured by massive transaction volumes.
- SSA and IRS: As the primary agencies responsible for large-scale federal benefit distributions and tax revenue collection, SSA and IRS represent high-stakes environments for proactive fraud detection. A pilot here could focus on identifying 'Payments Outside Normal Hours' and 'Frequent Manual Adjustments' patterns that are currently obscured by massive transaction volumes and often escape audit sampling.

Incorporate Mandatory Metadata Analysis Requirements

Update the Financial Audit Manual to require comprehensive metadata analysis as a standard audit procedure.

Update Regulatory Frameworks

Update federal audit regulations to recognize AI-driven metadata analysis as acceptable audit evidence under Generally Accepted Government Auditing Standards.

Conclusion

The research presented in this report reveals that opportunities exist to expand the current audit framework under the Financial Audit Manual procedures and Government Auditing Standards. While these standards provide systematic approaches to financial statement auditing, they prioritize the fairness and accuracy of financial reporting over the detection of fraud and abuse. Although the FAM includes fraud detection responsibilities within the audit framework, its primary mission focuses on ensuring financial statement reliability rather than comprehensive identification of fraudulent activities.

A critical limitation of current audit methodologies lies in their emphasis on reasonable assurance rather than assurance regarding material misstatements. This standard acknowledges that even properly executed audits cannot guarantee complete accuracy in audit opinions. The audit process remains heavily dependent on professional judgment and statistical sampling, both of which introduce inherent risks and potential blind spots in fraud detection capabilities.

Perhaps most significantly, federal audit processes lack systematic integration of advanced analytical technologies, including artificial intelligence and comprehensive metadata analysis. This technological gap represents an opportunity to enhance audit effectiveness in an era where transaction volumes and complexity continue to expand across government agencies.

The experimental component of this research, designed to replicate procedures performed by Inspectors General auditors, reveals substantial challenges at the substantive testing level. When auditors employ traditional sampling methods, only a limited portion of fraudulent transactions are generally selected for detailed analysis, creating significant probabilities that material fraud remains undetected and outside the scope of audit examination.

The experimental results demonstrate that traditional sampling approaches detected between 8 and 10 fraudulent transactions from a dataset containing 68 actual fraud cases, representing detection rates of only 11.8 percent to 14.7 percent. These findings indicate that 85-88 percent of fraudulent activity may escape detection through conventional audit sampling methodologies, even when such activity involves amounts exceeding established materiality thresholds.

In contrast, the machine learning approach successfully identified all 68 fraudulent transactions in the same dataset, representing complete detection of embedded fraud patterns. This comprehensive identification capability demonstrates that metadata-driven analytical approaches can achieve substantially higher fraud detection rates than traditional sampling methods, by examining entire transaction populations rather than statistical subsets.

The implications of these findings raise opportunities to improve federal financial oversight. The systematic under-detection of fraud through current methodologies suggests that significant amounts of taxpayer funds may be vulnerable to misuse without appropriate detection and remediation. The experimental evidence indicates that current audit designs can be enhanced to protect public resources and ensuring government accountability.

The demonstrated capabilities of machine learning approaches in fraud detection present an opportunity for federal audit methodology reform. The ability to analyze complete transaction populations using metadata characteristics offers a path toward more comprehensive and effective government oversight, without abandoning established audit standards and procedures.

However, the integration of advanced analytical capabilities into federal audit frameworks will require careful consideration of implementation challenges, including auditor training, technology infrastructure, regulatory adaptation, and cost-benefit considerations. The transition from sampling-based to population-based audit approaches represents a major shift in audit methodology, which must be managed thoughtfully to maintain audit quality while enhancing fraud detection capabilities.

Federal financial audit methodologies can be transformed to meet the challenges of contemporary government financial oversight. The current reliance on sampling-based approaches, while statistically sound for financial statement accuracy assessment, proves insufficient for comprehensive fraud detection in large-scale government expenditure environments. The integration of metadata analysis and machine learning capabilities offers a viable path toward enhanced audit effectiveness and improved protection of taxpayer resources.

The evidence presented in this study suggests that federal oversight agencies can prioritize the development and implementation of technology-enhanced audit methodologies that complement traditional approaches. Through such methodological evolution, federal financial auditing can achieve its mission of ensuring accountable and transparent use of public funds in an increasingly complex governmental financial environment.

Bibliography

Association of Certified Fraud Examiners. *Occupational Fraud 2024: A Report to the Nations.* 13th ed. Austin, TX: ACFE, March 2024.

Chief Financial Officers Act of 1990, Pub. L. No. 101-576, 104 Stat. 2838 (codified at 31 U.S.C. §§ 901–903).

Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, div. A, title I, § 101(f) [title VIII], 110 Stat. 3009-389 (codified at 31 U.S.C. § 3512 note).

Financial Audit Manual (FAM). Vol. 1. Washington, DC: U.S. Government Accountability Office and Council of the Inspectors General on Integrity and Efficiency, June 2024.

Fiscal Service Data Registry. Washington, DC: U.S. Department of the Treasury, Bureau of the Fiscal Service, January 31, 2025.

Government Auditing Standards (Yellow Book). GAO-24-106786. Washington, DC: U.S. Government Accountability Office, February 2024.

Government Management Reform Act of 1994, Pub. L. No. 103-356, § 405, 108 Stat. 3410, 3423 (codified at 31 U.S.C. § 331(e)).

Governmentwide Spending Data Model (GSDM). Washington, DC: U.S. Department of the Treasury, Bureau of the Fiscal Service, April 25, 2025.

Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified as amended in scattered sections of 5 U.S.C. app.).

Occupational Fraud Risk Management: 2018–2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud. GAO-24-105833. Washington, DC: U.S. Government Accountability Office, April 16, 2024.

Office of Management and Budget. *OMB Bulletin No. 24-01: Audit Requirements for Federal Financial Statements.* Washington, DC: August 2023.

Office of Management and Budget. *OMB Circular No. A-136: Financial Reporting Requirements.* Washington, DC: August 2023.

Payment Integrity Information Act of 2019, Pub. L. No. 116-117, 134 Stat. 113 (codified at 31 U.S.C. §§ 3351–3358).

Schmidt, Mark, Carol Hathaway, and Pablo Hernandez. *What Makes Government Workers Tick*. Washington, DC: The IBM Center for the Business of Government, 2012.

Technology Assessment: Artificial Intelligence in Federal Financial Management. GAO-21-519SP. Washington, DC: U.S. Government Accountability Office, June 2021.

USAspending.gov Data Archive. Washington, DC: U.S. Department of the Treasury, Bureau of the Fiscal Service, accessed August 5, 2025.

U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller). *Agency Financial Report, Fiscal Year 2024.* Washington, DC: November 2024.

U.S. Department of the Treasury, Bureau of the Fiscal Service. *Financial Report of the United States Government, Fiscal Year 2024.* Washington, DC: January 2025.

U.S. Government Accountability Office. *Assessing Data Reliability*. GAO-20-283G. Washington, DC: May 2021.

U.S. Government Accountability Office. *Financial Audit: Fiscal Year 2024 Financial Report of the United States Government.* GAO-25-105618. Washington, DC: January 2025.

U.S. Government Accountability Office. *Forensic Auditing: A Tool for Detecting Fraud*. GAO-09-867G. Washington, DC: July 2009.

About the Author

Dr. Irakli Petriashvili
Associate Professor, University of Georgia
Faculty Affiliate, Transparency and Governance Center
Rutgers University Newark

LI: Irakli Petriashvili
W: petriashvili.com
E: ip250@sussex.ac.uk

Dr. Irakli Petriashvili is a Certified Public Sector Auditor committed to advancing the architectural foundations of financial oversight through technology. At the University of Georgia, he teaches public administration, public sector auditing, and financial fraud detection courses. He serves as a faculty affiliate with the Transparency and Governance Center in the School of Public Affairs and Administration at Rutgers University–Newark, and as a Governance and Integrity Anti-Corruption Evidence (GI ACE) Fellow at the UK Centre for the Study of Corruption, University of Sussex, where he investigates how Supreme Audit Institutions can maximize their effectiveness through AI integration.

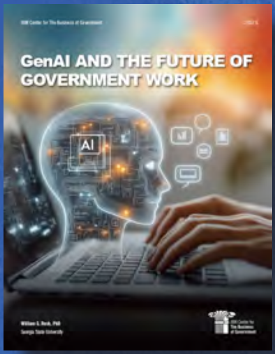
With extensive experience in government auditing, Dr. Petriashvili effectively bridges academic research and practical oversight, furthering public-sector accountability and integrity. His work operates at the nexus of public administration, anti-corruption, forensic auditing, and artificial intelligence, addressing systemic oversight challenges inherent in existing frameworks.

His research explores the potential of artificial intelligence, metadata analytics, and machine learning tools to strengthen governmental financial controls, facilitate earlier detection of irregularities, and detect corruption risks.

Dr. Petriashvili provides specialized training courses for public officials and develops effective tools aimed at preventing financial fraud and mitigating corruption risks in the workplace.

His initiatives have received support from reputable organizations including the U.S. Department of State, the International Monetary Fund (IMF), United Nations Office on Drugs and Crime (UNDOC), Swiss National Science Foundation, Swedish Institute and many others.

Recent Reports from the IBM Center for The Business of Government



GenAI and the Future of Government Work

by William G. Resh

Embedding Strategic Foresight into Strategic Planning and Management

by Bert George

RESPONSIBLE AI FOR PUBLIC EVALUATION
Harnessing AI to Strengthen Public Sector Decisions

Responsible AI for Public Evaluation

by Daniel Fonner

Practical Cyber Solutions for Managing Government Supply Chains

by Robert Handfield

Five Pillars of Effective Government

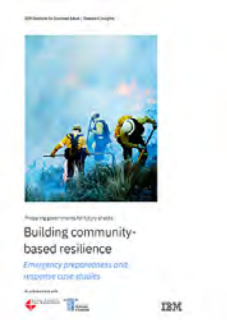
by Dan Chenok

Government's Digital DNA: Identity and Access Management for Public Sector Security

by Andrew Whitford

AI in State Government

by Katherine Barrett and Richard Greene


Building community-based resilience
Emergency preparedness and response case studies
IBM

Building community- based resilience

by Authors of Case Study

For a full listing of our reports, visit businessofgovernment.org/reports

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

IBM Center for
The Business
of Government