AICPA & CIMA

Fraud in the Public Sector

2024 Government Series

Contents

AICPA & CIMA

Introduction

Fraud is a vital concern at all levels of government as it can erode public confidence and trust. However, because fraud is inherently deceptive, discovering and reporting it can be a challenge. Once detected, investigation can then uncover the extent of the fraud.

Determining the existence of fraud requires an understanding of operational and reporting mechanisms, identification of potential risks and weak controls, and sometimes a stroke of luck. All levels of government (federal, state, and local) are experiencing misappropriations through many methods.

Fraud can be initially identified through an employee discovering inconsistencies, through both internal and external audits, and in some cases, through stakeholders and constituents who are experiencing difficulties. The finance and accounting professional is vital to discovering fraud, identifying its magnitude, understanding the failures in existing systems, and reporting properly to all stakeholders.

By the end of this report, you will understand both the unique ways fraud occurs in the public sector and your responsibility in addressing it. The report concludes with some actionable items you can do to deal with fraud in your entity.

AICPA & CIMA

What fraud looks like in government

Fraud is not limited to a finite list of activities or events. The varying functions and services that governments provide create many environments in which fraud can occur.

The COVID-19 pandemic contributed to significant and increasing pressures on all governments, particularly in the state and local sector. In order to execute their responsibilities with limited staffing or monetary support, switching often-antiquated IT systems from the office to a remote environment placed a strain on all governments.

The rapid pace of change taking place, along with personal difficulties like childcare and eldercare in the remote environment, created a perfect storm for fraud to increase. In the past few years, a spotlight has been placed on the growing number of fraudulent activities. Many of these fraud discoveries have come as a result of employees maintaining the integrity of their positions and implementing ethical, accurate, and efficient procedures and systems in a volatile and fast-paced environment.

The following case studies provide real-life occurrences of fraud. Though the methods of discovery, investigation, resulting improvements, and consequences are unique to each case, you will notice the cases share common threads.

This report will also provide you with actionable steps to help you begin or continue to minimise risk, no matter your area of responsibility.

Federal grant fraud

Across federal, state, tribal, territorial, and local governments, fraud can take many forms, including collusion, bid rigging, bribery, double invoicing, falsely adjusting inventory, and setting up 'ghost' companies or vendors to redirect funds. Considering the estimated outlays for both discretionary and mandatory federal grants for 2023 was $1.037 trillion[1] (about $3,200 per person in the United States), it is no surprise that grant fraud is on the rise.

Grant fraud in federal programmes ranges from falsifying applications and status reports to misusing funds and billing for work not performed. It can also overflow into other types of fraud and criminal activity that include family members and implicate innocent bystanders. For example, in February 2016, after receiving federal funding from the US Department of Energy (DOE), Department of Agriculture (USDA), and the National Science Foundation (NSF) to develop new asphalt technologies, Haifang 'Harry' Wen, Bin 'Ben' Wen, and Peng 'Jessica' Zhang were arrested for spending the research dollars on themselves.[2,3]

The defendants were charged with conspiracy to make false claims, conspiracy to commit wire fraud, a scheme to transfer funds obtained through specified unlawful activities (i.e., false grant applications), and conspiracy to commit money laundering.[4] In April 2018, charges against Harry Wen were dismissed after he signed a plea deal. He is still working as an engineer. In 2019, Bin Wen and Peng Zhang pleaded guilty and were convicted of conspiracy to commit wire and grant fraud.[5]

It is evident that careful planning went into the defendants' fraud scheme. Zhang incorporated United Environment & Energy, LLC (UEE) in 2003; Wen incorporated Advanced Technologies and Materials, LLC (ATM) in 2007; and in 2015, Wen established KEW Technologies, Inc. (KEW). Through UEE and KEW, the defendants submitted over 27 grant applications containing falsified documentation over multiple years to the NSF, DOE, and USDA for the Small Business Innovation Research and Small Business Technology Transfer programmes.[6]

---

[1] The White House, Office of Management and Budget, *Analytical Perspectives — Budget of the U.S. Government — Fiscal Year 2023,* Section: 'Special Topics', Chapter: 'Aid to State and Local Governments', table 14-1, 'Trends in Federal Grants to State and Local Governments', p. 206.

[2] *United States v. Wen*, 6:17-CR-06173 EAW, (W.D.N.Y. Dec. 21, 2018).

[3] Chad Sokol, 'WSU professor accused of fraud collected about 30 federal research grants', *The Spokesman-Review*, March 4, 2016.

[4] *United States v. Wen.*

[5] 'WSU assistant professor's brother pleads guilty to fraud', Staff Report, *Moscow-Pullman Daily News*, April 12, 2018.

[6] *United States v. Wen.*

In order to provide the supporting documentation for the grant applications, the defendants falsified proof of eligible investors, personnel, subject matter experts, and other funding sources. In the post-award phase, invoices should include the correct direct labour hours and personnel working on each project to reflect the programme's true progress.

The defendants claimed ATM as an investor of UEE. While ATM may have appeared to be a separate company from UEE, it was not a legitimate third-party investor. Ironically, ATM's business address was the same as UEE's, which was also the same as the defendants' residential address. Before ATM transferred funds to UEE as an investment, UEE had transferred funds to ATM in a larger amount, creating fake invoices. In addition to ATM, the defendants set up multiple 'sham' or shell investment companies that were 'supposed' to provide outside equity.[7]

In addition to the defendants using shell companies to falsely depict investors, they also falsified letters with the signatures of fictitious or unaffiliated individuals and a relative that may live in China or may not exist at all. They also submitted fabricated financial reports, budgets, personnel qualifications and contact information, entities, research facilities, matching funds, and investments. They also signed false certifications that the federal grantors relied on as part of the grant award process.[8]

---

[7] Ibid.

[8] Ibid.

Furthermore, the defendants budgeted time for research consultants at a much higher rate than stated within the New York Department of Labor's records. They also charged consultants' hours on invoices as employees, told employees to charge their time as they were directed regardless of the actual hours they worked, and falsified timecards that led to fraudulent invoices.[9]

Ultimately, the courts found that the defendants abused their positions of public and private trust, used their unique skills, were knowledgeable about the grant application and post-award requirements, and falsified their grant proposals. Most of the approximately $8.4 million that the defendants received though their two LLC companies in grant funds went to their personal use for salaries and their own investments.[10]

The diversion of the federal funds away from the intended purpose resulted in the deceleration of research programmes to develop high-tech innovations to benefit the public.[11] In addition to stealing taxpayers' dollars, the defendants also harmed the researchers' reputations by falsifying their credentials and misrepresenting their true relationship with the defendants' companies.[12]

The defendants were ordered to pay $5.5 million in restitution. Wen received a 33-month prison sentence, and Zhang was given 5 years of probation, including 6 months of house arrest.[13]

---

[9] Ibid.

[10] Ibid.

[11] U.S. Attorney's Office, Western District of New York, 'Husband And Wife Sentenced In Sc

[12] *United States v. Wen.*

[13] 'Husband And Wife Sentenced In Scheme To Defraud The United States'.

Preventing federal grant fraud

Detecting fraud related to grant awards can be challenging, but there are several safeguards and practices that can be adopted to prevent and identify fraudulent activities. Agencies should hire and train competent grant officers and specialists to analyse the eligibility of each grant applicant. They should also use predictive analyses and techniques to review historical facts and trends to determine the risks and probability of fraud related to grant awards. In the post-award phase, the federal grantor should consistently monitor milestones and grantee's spending to determine if funds are being expended in accordance with the agreed-upon budget and parameters of the grant programme.

The grantor should regularly review the grant award, including scrutinising financial and performance reports and matching them against grantee invoices before approving them. A review of the grantee's internal controls over the execution of the financial and programme grant activities can also help detect fraud. The development of a robust compliance programme including policies, disclosures, and review, along with risk assessments and internal controls that include segregation of duties and period audits, will provide additional detection and prevention avenues within the federal agency.

School district theft

While conducting the annual financial audit of Westside School District for the fiscal year ended June 30, 2016, Arkansas Legislative Audit (ALA) staff discovered discrepancies in revenue and cash disbursements during a review of credit card transactions. These required further investigation. ALA staff also interviewed current and former district employees and assessed internal control over the receipting and disbursement process for adequacy.

During an interview with ALA staff and Arkansas State Police on March 13, 2017, district treasurer Brandi Freeman admitted to the misappropriation of cash receipts remitted to her by district personnel. She also stated that she had used district credit cards to charge personal purchases and altered documentation to support these personal purchases. In addition, Freeman made online vendor payments from the district bank account to pay personal debts.[14]

Review of district financial records and interviews with district personnel revealed internal control over the receipting, depositing, and disbursement processes was deficient. Additionally, the superintendents and the board did not provide adequate fiscal oversight.

The district failed to establish and maintain adequate segregation of duties. As a result,

- bank statements were not reviewed by someone other than the employee issuing checks.
- the employee preparing checks and making deposits was also responsible for reconciling bank statements.
- invoices or other disbursement documentation was not reviewed for proper authorisation.
- purchase orders were prepared and/or altered by the employee issuing the checks.

The ALA found other deficiencies in the district's policies and procedures, including the following:

- Custody of district credit cards was not monitored; cards were passed from employee to employee without maintaining records.
- Credit card disbursements were not properly reviewed and authorised.
- The superintendent's signature stamp was not safeguarded.
- Activity fund and class sponsors were not provided computer-generated account balances.
- Employee complaints concerning issues with class and club account balances were ignored by management.
- Revenues and disbursements were miscoded in the accounting system.

---

[14] Chainee Bartlett, 'Former Westside School District Treasurer Arrested for Embezzlement', 5 News Online, September 7, 2017.

In addition to charging personal purchases to the district's credit cards, receiving reimbursements for personal purposes, and using district funds to pay for personal purchases and debt, Freeman deposited a check issued to a fictitious vendor into her personal bank account. ALA staff reviewed district financial records and transactions for the period July 1, 2013, through March 13, 2017, and discovered improper transactions totalling $178,391. In August 2018, Freeman was sentenced to 24 months in prison.[15]

Preventing school district fraud

In the aftermath of this fraud, safeguards were put in place to implement segregation of duties. Now, the district treasurer receipts money and issues check warrants. The payroll clerk balances monthly statements and the superintendent reviews bank reconciliations. All disbursements require a purchase order approved by the principal and superintendent prior to making a purchase. Credit cards are kept in the superintendent's and principal's office and may be checked out only with an approved purchase order. Credit card statements are opened, and purchase orders are matched to expenses.[16]

---

[15] Dave Hughes, 'Ex-school official ordered to repay $179,391', *Arkansas Democrat Gazette*, August 10, 2018.

[16] Arkansas Legislative Audit Investigative Report, 'Review of Selected Transactions Westside School District —Johnson County', Accessed April 11, 2024, https://arklegaudit.gov/downloadReport.php?id=IRSD20016.

An elected official's response to fraud in cash collection

Citizens elect individuals to positions of power expecting that fiduciary trust is the highest ethical standard they will exhibit. However, the Office of the New York State Comptroller issued a report on January 26, 2024,[17] to determine whether the justices and the Town of Marion board provided adequate oversight of the Justice Court to ensure cash collections were properly deposited, recorded, reported, and remitted. This fraud was committed by an individual directly overseen by an elected official.

The comptroller's findings identified that the justices failed to review reports submitted to New York State agencies to make sure all cases were properly reported and remitted. In addition, though the state auditor's office performs routine audits on a rotating basis, there was no review performed of bank reconciliations and other financial records to ensure collections were accounted for and to promptly identify discrepancies. Finally, the town failed to have an annual audit of the justice accounts.[18]

The failure of justices and the board allowed for a former court clerk to misappropriate over $59,000 of court funds. These misappropriations occurred between January 1, 2016, and May 31, 2021. In August of 2023, the former court clerk pled guilty to grand larceny in the second degree, corrupting the government in the second degree, tampering with records in the first degree, and official misconduct. The former court clerk was sentenced to six months in jail and to pay more than $59,000 in restitution. There were no penalties enacted to the board or judges and a corrective active plan was agreed to be put in place within 90 days.[19]

Preventing cash collection fraud

Detection of fraud in local government cash collections and disbursements is crucial for maintaining transparency, accountability, and public trust. Implementing and enhancing safeguards within cash collections begins with the separation of responsibilities in the collection of cash, recording transactions, and reconciling receipts.

Continuous monitoring is imperative to the success of fraud prevention in collections. Disbursements must be similarly monitored with extensive segregation of duties, reconciliations, and multiple layers of approval and authorisations. Vendor verification, bank account confirmations, and surprise reviews are necessary activities in the fight to prevent fraud.

---

[17] Office of the New York State Comptroller, 'Town of Marion — Misappropriation of Justice Court Cash Collections (2023M-149)', January 26, 2024.

[18] Ibid.

[19] Ibid.

State tax credits fraudulently used

In Pennsylvania, a couple used a sophisticated scheme to create fake companies, which then applied for tax credits fraudulently. A grand jury found the husband and wife were awarded $10.6 million worth of credits through the Keystone Innovation Zone and Research and Development tax credit programmes.

In this case, staff from the Pennsylvania Department of Revenue found inconsistencies in the tax credit applications submitted by certain business entities. Recognising the apparent criminal activity, the matter was referred to the Pennsylvania Office of Attorney General for investigation. That led to the convening of the grand jury that recommended the filing of criminal charges against individuals associated with those businesses.[20]

The actions of these individuals also led the Department of Revenue to implement an enhanced review process that is better equipped to detect fraudulent tax credit applications. This more rigorous review was automated to allow system edits and real-time data validations against specific data points throughout the process.

Additionally, staff from the department collaborated with lawmakers in the Pennsylvania General Assembly to advance legislation that strengthened the administration and transparency of Pennsylvania tax credit programmes.

Many of the recommendations from the grand jury that investigated the case were part of the legislation that was signed into law (P.L. 124, No. 25 in 2021). All these changes were made to detect and prevent fraud during the application phase, long before credits are awarded or sold.[21]

Preventing tax credit fraud

Prevention and detection related to fraud in tax credit programmes includes a combination of preventative efforts, such as edit checks and data validations in the online credit application, and vigilant detection procedures including audit and analytics. Each year, application controls are updated based on the prior year's data. The assignment of different individuals in the application, verification, and disbursement process, along with review of automated data analytics, has further strengthened controls over these programmes.[22]

---

[20] Pennsylvania Office of Attorney General, 'AG Shapiro Calls for Increased Tax Credit Program Oversight Following Grand Jury Investigation', Attorneygeneral.gov, December 5, 2019.

[21] Ibid.

[22] Ibid.

AICPA & CIMA

Who is responsible for detecting and preventing fraud?

Who is responsible for detecting and preventing fraud?

The short answer is **everyone**. The motto can no longer be 'That's not in my job description'. Elected officials, CFOs, clerks, and stakeholders all have a responsibility to detect and prevent fraud.

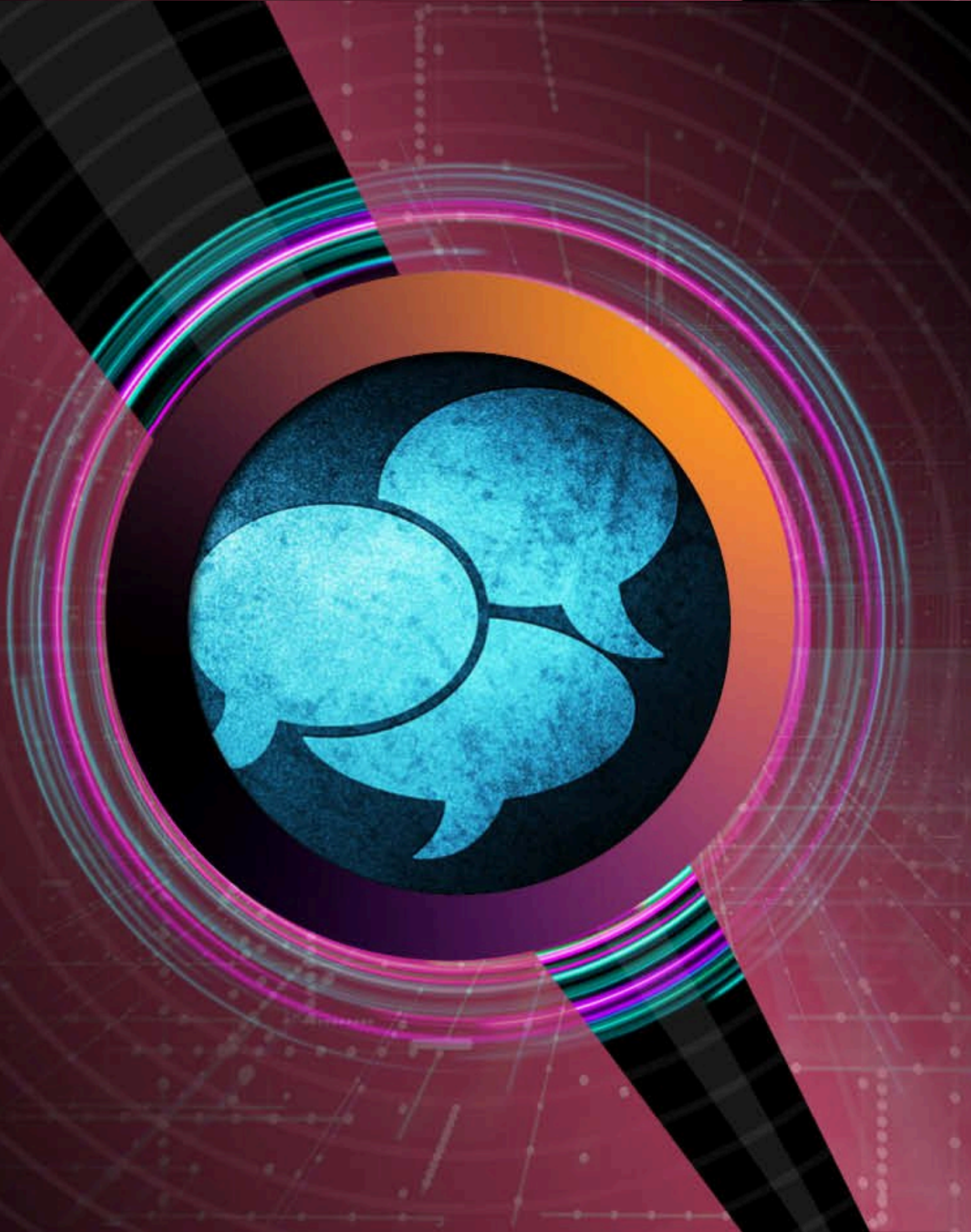
Fraud prevention in the public sector often involves a collaborative effort among both internal and external stakeholders. Each group plays a significant role in safeguarding public resources and maintaining public trust. Within the entity, internal audit departments hold a crucial role in assessing and monitoring internal controls, conducting audits to identify vulnerabilities, and recommending improvements in processes to prevent fraudulent activities.

Compliance and risk officers, formalised in some entities, monitor adherence to laws, regulations, and ethical standards and work to ensure compliance with legal requirements. The finance, analytical, and IT teams can work together to proactively identify patterns indicative of fraud. They can also take on the responsibility for developing and implementing advanced technologies to enhance fraud detection capabilities.

Externally, audit firms, law enforcement agencies, oversight agencies (for example, the Inspector General Office at the federal level), and whistleblower programmes have unique roles and responsibilities in preventing fraud. These include everything from investigating and pursuing legal actions to encouraging employees and citizens to report suspected fraud anonymously.

AICPA & CIMA

Starting and continuing the fraud conversation in your entity



Governments are accountable to the highest degree to themselves, their stakeholders, and citizens in the management of funds and resources. There are some initial steps to start the fraud conversation effectively.

Initiating a conversation within the public sector involves engaging key stakeholders regarding the culture of transparency and accountability. Bringing together representatives from identified departments, teams, functions, agencies, and others begins with a discussion on the importance of fraud prevention.

The impact on public resources, trust, and overall effectiveness of government operations should be included in these discussions. Initiating this dialogue can begin the path to developing and adopting more effective frameworks and policies to better safeguard the community.

In the cases discussed previously, controls and processes were strengthened to address fraud prevention and detection going forward. However, even increasing segregation of duties, developing and training people on policies, and expanding technological criteria and analysis cannot fully eliminate the risk of fraud — fraud will occur. But you can lessen its impact through diligence. The following are some actionable items that will assist you and your entity, regardless of where you are in your fraud prevention and detection journey.

Five ways you can address fraud

1. **Check the current status** of fraud activity and **identify** the risk in critical areas of performance and reporting. Review current policies and procedures, noting those that may be lacking or absent.
2. **Assess** recent audit findings, risk management reports, and complaints to identify areas at risk. Both internal and external oversight play a key role in this activity. If you are not already doing so, regularly conduct fraud risk assessments across various departments and processes.
3. **Determine three things** you can do **right now** to address fraud. Examples include performing a targeted fraud risk assessment, examining areas that have not been given attention due to their materiality, looking at trends, or considering feedback from data analysis or hotlines.
4. **Communicate** with others outside your department or entity and understand their areas of concern. Build on others' proven experience. The fostering of collaboration leads to best practices across the entity.
5. **Educate and train** employees and officials at all levels about fraud risks, detection methods, and the importance of reporting suspicious activities. This includes ensuring staff understand their role in preventing fraud. The focus on training in the detection and ramifications of fraud creates an army of individuals able to 'do the right thing always'.

The incorporation of these strategies, along with others, lays the foundation of an initiative-taking approach to fraud prevention, creating a culture of integrity, transparency, and accountability within the public sector.

AICPA & CIMA

Summary

As this report shows, fraud has no limits. Fraud detection and prevention play a crucial role in the public sector's management of the trust placed in it by citizens.

Implementing robust fraud detection systems helps safeguard public funds, reduce financial losses, and maintain trust in government operations. Various techniques such as data analytics, generative artificial intelligence (AI), and strategic risk assessments are used to identify irregularities and potentially fraudulent activities. An initiative-taking approach allows governments to detect and mitigate fraud before it can cause significant harm and loss, thereby preserving the effectiveness of public services and programmes.

Once a robust fraud detection and prevention system is in place, there are several positive outcomes. First and foremost, it leads to increased transparency and accountability, as citizens can have confidence that their tax dollars are being used efficiently and responsibly. Secondly, the government can optimise resource allocation by redirecting funds away from fraudulent activities and towards legitimate and essential services. Moreover, a successful fraud prevention system fosters a culture of compliance and discourages fraudulent behaviour, contributing to the overall effectiveness of public programs. Overall, the implementation of advanced fraud detection measures is pivotal in ensuring the responsible and efficient use of public resources.

AICPA & CIMA

Lead authors and acknowledgements

Authors

Lori A. Sexton, CPA, CGMA,
Associate Technical Director, Management Accounting
The Association of International Certified Professional Accountants

Scott M. Adair, CPA, CGMA
Chief Financial Officer
Rochester Genesee Regional Transportation Authority

Ross Baldwin, CPA, CGMA, CIA, CFE
Senior Auditor
Arkansas Legislative Audit

Carrie Hug, CPA, CGMA, CGFM, CFE
CFO, Federal Motor Carrier Safety Administration
US Department of Transportation

John Kaschak, CPA, CGMA, CISA
Chief Accounting Officer
PA Department of Budget

Acknowledgements

We would like to thank contributors to the AICPA's Government and Performance Accountability CGMA Advisory Group:

Ravenna Bohan, CPA
John Gaspich, CPA, CFE, CRMA, CGFM, CHIAP, ML, MPA
Carrie Kruse, CPA, CGMA
Suzanne Lowensohn, CPA, CGMA
Jeff Parkison, CPA, CGMA
Ashley Stallings, CPA

Publication date: June 10, 2024

aicpa.org

About the Association of International Certified Professional Accountants and AICPA & CIMA

The Association of International Certified Professional Accountants® (the Association), representing AICPA® & CIMA®, advances the global accounting and finance profession through its work on behalf of 689,000 AICPA and CIMA members, students and engaged professionals in 196 countries and territories. Together, we are the worldwide leader on public and management accounting issues through advocacy, support for the CPA licence and specialised credentials, professional education and thought leadership. We build trust by empowering our members and engaged professionals with the knowledge and opportunities to be leaders in broadening prosperity for a more inclusive, sustainable, and resilient future.

The American Institute of CPAs® (AICPA), the world's largest member association representing the CPA profession, sets ethical standards for its members and US auditing standards for private companies, not-for-profit organisations, and federal, state, and local governments. It also develops and grades the Uniform CPA Examination and builds the pipeline of future talent for the public accounting profession.

The Chartered Institute of Management Accountants® (CIMA) is the world's leading and largest professional body of management accountants. CIMA works closely with employers and sponsors leading-edge research, constantly updating its professional qualification and professional experience requirements to ensure it remains the employer's choice when recruiting financially trained business leaders.

The information and any opinions expressed in this material do not represent official pronouncements of or on behalf of the AICPA, CIMA, or the Association of International Certified Professional Accountants. This material is offered with the understanding that it does not constitute legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The information contained herein is provided to assist the reader in developing a general understanding of the topics discussed but no attempt has been made to cover the subjects or issues exhaustively. While every attempt to verify the timeliness and accuracy of the information herein as of the date of issuance has been made, no guarantee is or can be given regarding the applicability of the information found within to any given set of facts and circumstances.

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.

AICPA & CIMA

Thank you for reading

Fraud in the Public Sector