SUMMIT BUSINESS SOLUTIONS LLC

Fractional CFO | Bookkeeping | Cost Reduction Consulting

Government & Nonprofit Internal Controls Guide

A Practical Framework for States, Counties, Cities, and School Districts

to Reduce Fraud, Waste, and Abuse of Public Trust

---

13 Areas of Risk, Built from Real Public-Sector Cases

Inmate Trust Funds · Payroll & Ghost Employees · Procurement & Bid-Rigging · Grant Funds
Vehicles & Equipment · Off-Duty Law Enforcement · Land Deals & Conflicts of Interest · Credentials

Travis Hawk, MBA
travis@travishawk.com · 405-850-4776 · travishawk.com
Edmond, Oklahoma

Why This Guide Exists

Every case in this guide is real, sourced from Department of Justice press releases, state auditor reports, Inspector General findings, and investigative journalism. Together they show the same pattern across states, counties, cities, and school districts of every size: the fraud is rarely sophisticated. It survives because one person had too much unchecked access, because a policy existed only on paper, or because raising a concern felt more dangerous than staying quiet.

This guide is organized by the areas where public entities most often lose money — from a single jail commissary account to a $250 million federal grant program. Some sections will apply directly to your organization. Others may not apply today but are worth knowing, because the same structural gaps show up in different departments wearing different names.

> **One important caveat before you read further:**
> Internal controls don't guarantee fraud will never happen. Even the most sophisticated federal programs, with dedicated oversight staff, have been defrauded of hundreds of millions of dollars. What controls do is reduce the opportunity, increase the chance of early detection, and limit the damage when something goes wrong. That's the honest, professional standard this guide is built around — not a promise nobody can keep.

Items marked **KEY** are the highest-value controls in each section — the ones most likely to have caught the real cases described here before the loss grew large. If your organization can only act on a handful of items, start there.

A. Governance, Culture & Hiring

Every case in this guide traces back to the same starting condition: one person with unchecked access and nobody expected to check.

- Run background checks and verify references for any position with access to cash, inmate funds, payroll, procurement, or public property.
- Require all employees, and especially finance/accounting staff, to take real, uninterrupted vacation time each year — one of the single best fraud-detection controls that exists, since most schemes require daily maintenance to conceal. **KEY**
- Put policies in writing and require signed acknowledgment — don't rely on verbal understanding of what is and is not permitted.
- Establish and publicize a confidential whistleblower reporting channel, and make clear — in writing and in practice — that reports will not result in retaliation. Several of the largest cases in this guide were flagged internally years before they were stopped, but staff faced pressure to stay quiet. **KEY**
- Hold periodic manager-level reviews of internal controls; don't treat a policy as "done" once it's written.
- Ensure the person or office responsible for fraud, waste, and abuse oversight (Inspector General, Auditor, Comptroller) has genuine independence from the officials and departments it may need to investigate.

B. Cash, Banking & Digital Payments

Cash and payment fraud rely on one thing above all: a missing second set of eyes.

- Require dual signatures or dual electronic approval on all checks, wires, and ACH transfers above a set threshold, with no informal exceptions.
- Require independent call-back verification, on a known phone number, for any request to change payment or banking instructions — never trust the number or account provided in the request itself. **KEY**
- Prohibit the use of Cash App, Venmo, Zelle, or any peer-to-peer consumer payment app for any vendor, employee, or program payment. These apps carry no dual-approval capability, no vendor master file, and often no verified legal identity behind the receiving account — exactly the gap that let a dealership employee in one documented case reroute refunds to a personal account undetected. **KEY**
- Reconcile bank statements independently of whoever has transaction entry access, and have that reconciliation reviewed by a second person, not just filed.
- Conduct unannounced cash counts wherever public money is collected in person — clerk windows, permit offices, court fee counters, jail intake.
- Use lockboxes for mailed payments where volume justifies it, and ensure the person opening mail is not the same person who posts payments.

C. Payroll & Ghost Employees

A ghost employee is a fictitious or no-longer-real person kept on payroll to divert public funds. It is illegal in every state and, in California, carries a lifetime ban from holding public office on conviction.

> **How it's been caught — a Department of Defense case study**
>
> An anonymous tip flagged that timesheets carried the approval signature of a manager who had retired a year earlier. Auditors compared the signature name against the current HR employee list and confirmed he was gone — yet paychecks were still going out. The entire scheme was exposed by one simple cross-reference.

Ghost employee schemes are especially common in school district administration, where seasonal coaching and support staff create high turnover and administrative autonomy — a supervisor adding a “coach” who never reports for duty is a recognized pattern nationally.

- Cross-reference every name on the payroll register against the current HR personnel file monthly, not just at year-end audit. **KEY**
- Segregate who can add or edit an employee record in the payroll system from who approves and releases the payroll run — the same person should never do both. **KEY**
- Require in-person or notarized identity verification (government-issued ID, Social Security card) on file before any new hire is entered into payroll.
- Watch for duplicate or near-duplicate bank account numbers across different employee records.
- Verify any direct deposit account change directly with the employee by phone or in person, never through email alone — a common scheme redirects a real or recently terminated employee's pay to a fraudster's own account. **KEY**
- Terminate system and payroll access immediately upon separation — don't let this lag administratively.
- Physically confirm presence periodically for positions not routinely seen in person (site visits, badge or biometric access logs).

D. Vendor Fraud & Fake Vendors

A fake vendor is a shell entity, often set up by an employee, used to submit invoices for goods or services never delivered.

> **How it's been done — a nonprofit case**
>
> A low-level accounts receivable employee created fake companies, assigned them vendor numbers in the organization's own system, and submitted invoices for work that was never performed — going undetected for five years and totaling $1.48 million, despite the employee holding a junior position.

- Run an automated match of every vendor address and bank routing/account number against the full employee address and payroll file, flagging any overlap for mandatory investigation before payment is released. **KEY**

- Require independent approval before any new vendor is added to the system, separate from whoever processes payments to that vendor.
- Separate the person who enters bills from the person who approves and releases payment on them.
- Periodically audit for vendors with no verifiable physical presence, P.O.-box-only addresses, or suspiciously regular/round invoice amounts.
- Rotate which employees handle vendor setup versus vendor payment approval.
- Require supporting documentation — contract, purchase order, receiving confirmation — before any invoice is paid, and periodically verify a sample of vendor balances directly with the vendor.

E. Procurement & Bid-Rigging

Bid-rigging distorts the competitive process that is supposed to protect taxpayers, and it is one of the U.S. Department of Justice's standing enforcement priorities through its Procurement Collusion Strike Force.

A case close to home — Oklahoma transportation contracts, $100 million+

Four erosion control company owners and managers pleaded guilty to a conspiracy running from 2017 to 2023, targeting over $100 million in publicly funded Oklahoma Department of Transportation contracts. Competitors took turns winning contracts by geographic area, submitting intentionally high "sham" bids or simply declining to bid whenever it wasn't their turn. One defendant had worked for the Oklahoma DOT for 15 years before moving to the industry side — a reminder that insider knowledge of the bidding process makes collusion easier to arrange and harder to detect.

In a separate federal case, a contractor paid over $100,000 in bribes — including cash, automobiles, and firearms — to two Army contracting officials to steer $19 million in contracts, then separately collected $723,333 in kickbacks from a subcontractor in exchange for assigning that work. In a Maryland IT contracting case, insiders nicknamed their kickback scheme the "Vic tax" — a level of casual normalization worth noting for how quickly unchecked kickbacks become treated as routine.

- Analyze bid patterns over time for the same group of vendors — rotation of winners by geography or job type, and bids that consistently land 'just below' a competitor, are statistical red flags, not coincidence. **KEY**
- Separate who writes bid specifications, who evaluates submitted bids, and who approves the awarded contract — no single employee should control all three stages. **KEY**
- Require disclosure of any prior employment relationship between procurement staff and bidding companies.
- Benchmark contract prices against regional and historical cost data, not just against the bids received in a given round.
- Watch for unusually narrow or burdensome bid specifications that appear tailored to a single, pre-selected bidder.
- Report suspicious bidding patterns to the DOJ's Procurement Collusion Strike Force (justice.gov/procurement-collusion-strike-force), a standing federal resource built specifically for this.

F. Grant Funds & Nonprofit Program Reimbursement

This is the highest-dollar risk category in this entire guide, and the mechanism has been laid out in exceptional detail by federal prosecutors in a single case.

Feeding Our Future (Minnesota) — $250 million, the largest pandemic-era fraud scheme in U.S. history

A nonprofit sponsor recruited 250+ "meal sites" that claimed to serve thousands of children daily, often within days of being formed. Attendance rosters were fabricated using names pulled from a random-name-generator website; one roster listed 2,040 children, of whom only 20 names matched real students in that school district. Fake ages were generated with an Excel formula. One restaurant that previously had a few dozen customers a day and $500–600 in daily sales suddenly claimed to serve 2,000–3,000 meals daily, seven days a week. The sponsor collected $18 million in administrative fees for "monitoring" sites it was defrauding, and employees took kickbacks disguised as "consulting fees" paid to shell companies they had set up themselves. Funding ballooned from $3.4 million in 2019 to nearly $200 million in 2021. State officials had flagged suspected fraud internally years earlier but continued approving payments, citing fear of lawsuits and public backlash. Federal waivers had also suspended standard on-site inspection requirements right as funding volume exploded, removing what little mandatory monitoring existed.

- Never disburse based on self-reported attendance, service, or meal counts alone — require independent, random-sample verification against actual enrollment or attendance records from a separate, unaffiliated source. **KEY**
- Flag disproportionate year-over-year growth automatically — any organization whose funding volume jumps 10x or more should trigger mandatory enhanced review, not routine processing. **KEY**
- Never waive on-site inspection requirements wholesale, even during a declared emergency — build a reduced-but-not-eliminated inspection tier for crisis situations instead of an all-or-nothing suspension. **KEY**
- Compare claimed volume against plausible operational capacity — prior revenue history, staff size, physical space — before approving; a sudden, implausible jump in claimed service volume is the clearest and easiest signal to catch.
- Treat "consulting fees" paid to newly formed, employee-linked entities as an automatic audit trigger.
- Insulate the fraud-review and compliance function from political and reputational pressure. Build a reporting structure — an independent Inspector General or equivalent — so staff who flag suspected fraud early are not overruled or silenced by concerns about public or political backlash. **KEY**

G. Jails & Corrections — Inmate Trust & Commissary Funds

Inmate trust and commissary accounts are uniquely vulnerable: they often sit outside the normal county treasury, are reconciled against a third-party vendor's separate system, and in several documented cases were controlled by a single employee.

Real losses, same structural gap

A Knox County, Illinois jail administrator — the only employee with access to the account — diverted more than $200,000 in commissary kiosk deposits over six years, later forging reconciliation entries during a software upgrade. In New Orleans, a forensic audit by a newly hired CFO uncovered two simultaneous schemes: an inmate accounts clerk and her supervisor skimmed roughly $4,000 a month (nearly $90,000 total) from public deposits, disguising it with falsified journal entries and replacement check disbursements; separately, a grants employee funneled $75,000 through a fake business. A Starke County, Indiana jail matron made 19 unauthorized withdrawals from inmate accounts totaling over $20,000. An Elkhart County, Indiana booking specialist created more than 600 fraudulent debit cards drawn against former inmates' accounts, totaling $27,239 — caught only when a secretary noticed a $22.25 discrepancy on one account.

- Never allow a single employee to be the sole person with access to the inmate trust/commissary account. Require a minimum of two people for reconciliation, with one independent of daily transaction entry. **KEY**
- Reconcile the jail's internal ledger against the third-party commissary vendor's own records monthly, performed by someone outside the daily commissary operation — several of these schemes exploited exactly this reconciliation gap. **KEY**
- Require independent verification of any release debit card issued to a departing inmate, cross-checked against the actual release date and balance.
- Audit dormant or former-inmate accounts specifically — the Elkhart case was only caught because someone happened to check a released inmate's account.
- Require dual sign-off on any manual journal entry adjusting an inmate trust balance.
- Have an outside auditor perform a full reconciliation of the inmate trust fund at least annually, independent of jail administration.

H. Public Vehicles, Equipment & Property Use

Beyond vehicles, this covers tools, heavy equipment, materials, and even employee labor time diverted to personal or private business use.

How it's happened

A Mississippi road foreman and supervisor entered a private contract with a landowner to tear down and remove debris — using county equipment and county employees to do the work, then pocketing the payment personally. A Johnson County, Iowa Conservation Department superintendent took $1,600 in lumber from the county sawmill for personal woodworking projects, and staff reported being routinely directed to help him on county time. An Atlanta deputy fire chief was alleged to have used city equipment and property to run his own private company. A Chicago city employee used their government title, email, and office equipment to help their own outside business secure permits — resulting in $16,000 in ethics fines.

- Require a written, signed acknowledgment of a no-personal-use policy covering all vehicles, tools, equipment, and materials — including surplus and disposal items, closing the 'it was just going to be thrown away' excuse. **KEY**
- Maintain equipment checkout/return logs for anything that leaves the yard or shop — heavy equipment, power tools — with a named employee, stated purpose, and expected return. **KEY**
- Reconcile materials/supply usage (lumber, gravel, fuel) against actual job or work-order numbers monthly.
- Prohibit supervisors from directing subordinates to assist with personal projects, and provide a confidential channel for employees to report being asked to do so without fear of retaliation. **KEY**
- Conduct random, unannounced equipment audits rather than relying solely on an annual scheduled inventory.
- Extend the no-personal-use policy explicitly to computers, email, and government letterhead or title — using a government email address or job title to conduct outside business is the same category of misuse as taking a piece of equipment home.

I. Off-Duty Law Enforcement & Private Security

A nationwide investigation by CBS News and the Howard Center for Investigative Journalism reviewed off-duty employment policies at 100+ law enforcement agencies and found fewer than one in four check an officer's internal disciplinary history before approving them for off-duty security work.

Documented patterns

A Washington, DC officer worked as an armed grocery-store security guard on 193 separate occasions over nearly two years while simultaneously reporting himself on-duty and patrolling his police district — a $45,000-plus fraud caught through the store's own timecard records. A Florida lieutenant claimed to work extra-duty security jobs while GPS on his city vehicle showed him at home, and at times in a different county entirely; in at least one instance he was paid twice for the same block of time. A Florida officer faked 79 off-duty shifts for a housing development that, investigators found, never actually had a contract with him. A New Orleans sergeant's payroll records showed him ‘working’ 4,529 hours in a year — over 12 hours a day, every day, with no days off. In Dallas, an off-duty coordinator told a hiring company he'd pay officers $75/hour but only passed along $45/hour, pocketing the difference — and the department's own rules permitted coordinators to distribute cash directly with no oversight of either number.

- Route all off-duty security pay through the department, never direct cash from the hiring business to the officer — this single structural fix closes the coordinator-skimming gap seen in multiple documented cases. **KEY**
- Track and cap total combined hours (regular duty plus off-duty plus overtime) per officer per day and week, with automatic flags for implausible totals. **KEY**
- Use GPS/AVL tracking on department vehicles, cross-referenced against claimed work location and off-duty job site.
- Require the hiring business to confirm hours directly with the department rather than accepting an officer's self-reported invoice, and require a written, on-file contract for every off-duty assignment.
- Check disciplinary history before approving off-duty work, and automatically suspend off-duty privileges during any active internal investigation. **KEY**
- Conduct independent, random audits of off-duty timecards against actual duty schedules rather than relying on a self-certifying honor system.
- Do not permit quiet resignations in lieu of documented discipline for financial misconduct — findings should go on record with the relevant state certification board to prevent an officer from being quietly hired at a new agency before the issue surfaces.

J. Travel, Expense Reports & Hospitality

A state comptroller's office maintains a standing list of recurring audit findings in this category — meaning these aren't rare surprises, they're a known, recurring pattern across public entities.

Documented recurring findings include: alcohol purchased with taxpayer dollars, payment of spousal or other non-employee travel with public funds, extension of trips after a conference for personal reasons at public expense, and reimbursement claims for expenses already charged to a government credit card. A separate city internal audit found lodging rates averaging 44% above the federal GSA benchmark rate with no enforced deviation range, and no mechanism to track or prevent misuse of airline e-credits from canceled flights.

- Require pre-approval for conference/travel attendance, with a written travel policy that explicitly lists non-reimbursable expenses — alcohol, entertainment, spousal or non-employee travel — rather than relying on a vague 'reasonable expenses' standard. **KEY**
- Benchmark lodging reimbursement against the federal GSA per diem rate for the destination, with a defined and enforced maximum deviation.
- Require original itemized receipts, not just a credit card slip, for every expense submitted.
- Have the governing board, or a designated independent auditing officer, review and approve travel claims before payment — not just a supervisor who may have approved the trip in the first place. **KEY**
- Track and require documentation for any trip extension beyond the conference dates, and prohibit charging the extension to public funds.
- Require any credit for a canceled ticket to be returned to the agency's account, with a tracking mechanism to confirm it was applied to a future business trip, not a personal one.

K. Land Acquisitions & Conflicts of Interest

This scheme involves an insider tipping off a friend or associate to buy land ahead of a known future government acquisition, then flipping it to the government at a large profit.

A textbook case — Global Transportation Hub land flip

A government-owned industrial park needed land for a highway interchange. A businessman's company bought and sold the land in a single day, making a $6 million profit. The buyer held it about a year and sold it to the government authority for another $5 million profit. The authority ultimately paid $103,000 per acre — while the transportation ministry's own appraisal said the land was worth $30,000–35,000 per acre, and the authority's own separate appraisal said $51,000–65,000 per acre. The official responsible for approving the purchase had an undisclosed landlord/tenant relationship with the seller's family, surfacing only after journalists began asking questions. His justification for the inflated price: the seller had his own appraisal showing the land was worth more — which he accepted over his own agency's professional appraisal.

- Require at least two independent, arm's-length appraisals before any land acquisition, with a mandatory written explanation on file if the purchase price exceeds either appraisal by more than a defined percentage. **KEY**
- Require mandatory conflict-of-interest disclosure and recusal for any official with a personal, family, or business relationship — including landlord/tenant — to a seller, buyer, or intermediary, disclosed before any vote, not after the fact. **KEY**
- Review chain-of-title on any parcel being acquired for a public project going back at least 24 months; a same-day flip or rapid resale is a major red flag warranting additional scrutiny.
- Restrict officials, employees, and immediate family from purchasing property within a defined radius of a known or planned public project for a set period after the project becomes internally known.
- Separate the person(s) who know a project's planned route or location from the acquisition/negotiation team, or require an independent second signer with no prior route knowledge to approve final price.
- Require board or commission approval with the full appraisal spread disclosed publicly before authorizing any purchase.

L. Credential Fraud & Salary Verification

Salary schedules in government and education are directly tied to degree level, which is precisely the incentive diploma mills are built to exploit.

The national story — Pittsburg, Kansas

A newly hired high school principal's $93,000 salary was tied in part to a master's and doctorate from an unaccredited online “university.” Six student journalists on the school newspaper — not the district's own hiring process — discovered the institution had no verifiable accreditation, physical address, or legitimacy, and was widely identified as a diploma mill. She resigned before her first day. The superintendent's own words: ‘As superintendent, I feel like I let the teachers and the students down. I publicly admit that... the district would probably be making changes to its vetting process.’

A congressional hearing cited an estimate from the National Council for Accreditation of Teacher Education that one in six education doctorates may be fraudulent. A U.S. Senate investigation separately found federal agencies had reimbursed employees for degrees from unaccredited schools.

- Never accept a diploma, transcript, or self-reported degree as verification — require primary-source verification directly from the institution's registrar or a third-party credential verification service before any salary schedule advancement is processed. **KEY**
- Verify accreditation status independently at the time of the salary decision, not just at hire — confirm the institution was accredited both when the degree was allegedly earned and remains verifiable now through the U.S. Department of Education's accredited institutions database. **KEY**
- Separate the person processing a pay increase from the person who verified the credential.
- Re-verify credentials at any promotion into a higher trust/pay tier (teacher to principal, principal to superintendent), not only at initial hire.
- Cross-check institution names against a maintained diploma mill list, such as Oregon's Office of Degree Authorization, considered the most authoritative available.
- Periodically re-audit existing staff credentials, not only new hires — several documented cases involved a fraudulent credential quietly drawing a higher salary for years before anyone checked.

M. Systems, Access & Independent Oversight

Every category in this guide is easier to prevent, and far easier to detect early, when independent oversight is genuinely independent.

- Maintain a list of who has access to each financial system — banking, payroll, procurement, inmate trust — and review it quarterly.
- Deactivate system access immediately upon separation; use unique logins for every user, never a shared login, so any action traces to a specific person.
- Enable two-factor authentication on all financial and payroll systems.
- Maintain an audit trail or change log in every financial system and periodically review it for unusual edits, deletions, or backdated entries.
- Have the organization's books and, where applicable, program compliance reviewed by an outside auditor at least annually — for entities too small to fully separate duties internally, this is the single highest-value control available. **KEY**
- Ensure the Inspector General, Auditor, or Comptroller function reports independently of the officials and departments it may need to investigate, with statutory or charter protection from being defunded or overruled in retaliation for unfavorable findings. **KEY**
- Publicize a fraud, waste, and abuse reporting hotline and require every new employee to be told about it during onboarding.

The Bottom Line

Most public-sector fraud does not happen because someone found a brilliant way around the system.

It happens because there was no system to get around — one person with sole access to an account, one policy that existed only on paper, one employee who raised a concern and was told to stay quiet. The scale ranges from a single jail commissary account to a $250 million federal program, but the structural gap is nearly always the same.

Internal controls cannot eliminate every risk. But they can make sure one bad decision, one unverified credential, or one unsupervised account doesn't turn into a loss the public can't afford and won't forgive.

Self-Assessment Scorecard

Eighteen questions, one or two from each area of this guide. Answer honestly — this is a diagnostic, not a test. Score 2 points for Yes, 1 for Partially, 0 for No.

Control	Yes	Partial	No
Employees with access to cash, inmate funds, payroll, or procurement undergo background checks, and finance staff take real vacation time each year.	☐	☐	☐
We have a confidential whistleblower channel, and staff are told during onboarding that reports will not result in retaliation.	☐	☐	☐
Peer-to-peer payment apps (Cash App, Venmo, Zelle) are explicitly prohibited for any vendor, employee, or program payment.	☐	☐	☐
Payroll registers are cross-referenced against current HR personnel files monthly, and the same person cannot add an employee and approve payroll.	☐	☐	☐
Vendor addresses and bank details are automatically checked against employee address and payroll records.	☐	☐	☐
We analyze bid patterns over time for rotation or suspicious patterns among the same group of vendors.	☐	☐	☐
Grant or program reimbursements are verified against independent attendance/service records, not self-reported counts alone.	☐	☐	☐
No single employee has sole access to the inmate trust/commissary account, and it is reconciled against the vendor's own records monthly.	☐	☐	☐
We require a signed no-personal-use policy covering all vehicles, tools, equipment, and materials, including surplus items.	☐	☐	☐
Off-duty law enforcement pay is routed through the department, never distributed as direct cash by a coordinator.	☐	☐	☐
Officers' disciplinary history is checked before approving off-duty work, and off-duty privileges are suspended during active investigations.	☐	☐	☐
Our travel policy explicitly lists non-reimbursable expenses (alcohol, spousal travel, entertainment) rather than a vague standard.	☐	☐	☐
Lodging reimbursement is benchmarked against the federal GSA rate with an enforced maximum deviation.	☐	☐	☐
Land acquisitions require at least two independent appraisals, with mandatory disclosure if the purchase price exceeds either one.	☐	☐	☐
Officials disclose and recuse from any personal or business relationship with a party to a land or contract transaction before any vote.	☐	☐	☐
Academic credentials are verified directly with the institution before any salary schedule advancement is processed.	☐	☐	☐
System access is reviewed quarterly, with unique logins for every user and immediate deactivation upon separation.	☐	☐	☐
Our Inspector General, Auditor, or Comptroller function is genuinely independent and cannot be defunded or overruled in retaliation for findings.	☐	☐	☐

32–36 points	20–31 points	Below 20
Strong control environment	Moderate risk — worth a closer look	Significant opportunity for improvement

A "Partially" or "No" answer isn't a failing grade — it's simply where the highest-value conversation about your organization should start.

Want to Talk Through Where Your Organization Stands?

Summit Business Solutions works with public entities and nonprofit boards on fractional CFO support, financial oversight, and internal control reviews built around exactly this framework.

Travis Hawk, MBA — Summit Business Solutions LLC
405-850-4776 · travis@travishawk.com · travishawk.com