SUMMIT BUSINESS SOLUTIONS LLC

Fractional CFO | Bookkeeping | Cost Reduction Consulting

Small Business Internal Controls Guide

A Practical Framework for Owners and Bookkeepers

to Reduce Fraud and Strengthen Financial Oversight

For Any Industry, Any Size Business

Cash & Banking · Payroll · Receivables & Payables · Inventory & Fixed Assets
Segregation of Duties for the One-Person Accounting Department · Systems Access · Insurance

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

Why This Guide Exists

Most small business fraud doesn't involve a criminal mastermind. It involves one trusted person — often a bookkeeper — who ends up with too much unchecked access: entering the bill, cutting the check, reconciling the bank statement, and recording the entry, all without anyone else looking over their shoulder. That's not usually anyone's fault. It's just how small businesses grow. Nobody sat down and designed it that way.

This guide is built to work across any industry — retail, services, construction, medical, nonprofit, professional practice — for owners who want to know what to check, and for bookkeepers who want a framework to bring to the businesses they support.

> **One important caveat before you read further:**
> Internal controls don't guarantee fraud will never happen. Even the best-run companies in the world experience it. 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 this guide — the ones most likely to catch or stop a problem in a business too small to fully separate duties. If you can only act on a handful of items, start there.

A. Governance, Culture & Hiring

Controls start with people, not spreadsheets. A business that is visibly engaged with its own numbers prevents far more loss than one relying on paperwork alone.

- Bond key financial employees — anyone with check-signing authority, banking access, or payroll access.
- Check references and past employers before hiring anyone who will handle money or financial records.
- Run a background check for any role handling cash, banking, or payroll.
- Put financial policies in writing — don't rely on a verbal understanding of who can do what.
- Require all employees, and especially your bookkeeper or accounting staff, to take real, uninterrupted vacation time every year. This is one of the single best fraud-detection controls that exists — most embezzlement schemes require daily maintenance and unravel the moment someone else touches the books. KEY
- Communicate clearly and repeatedly that the owner is engaged and reviewing financials. Visible oversight deters more fraud than any single technical control.
- Hold a brief, periodic review of controls with your bookkeeper or accountant — don't "set and forget" the system once it's in place.
- Define, in writing, exactly what your bookkeeper is and is not authorized to do — for example, they can enter bills but not approve payment; they can reconcile the bank statement but not also initiate transfers. KEY

B. Cash & Banking Controls

Cash and wire fraud rely on one thing above all: a missing second set of eyes. Every control below exists to put one back.

- Have business mail addressed to a P.O. box, or have the owner personally open and review incoming mail before it's distributed.
- Review the business's cash position at least weekly — don't just glance at the checking account balance.
- Bank reconciliations should be reviewed — not just prepared — by someone with zero access to cash. In a one-bookkeeper business, this means the owner personally reviews the actual bank statement directly from the bank, not just the bookkeeper's reconciliation report. KEY
- Restrict online banking access: give the bookkeeper entry-level or view-only access where possible, with the owner or a second person required to release payments.
- Require dual approval and independent call-back verification on any wire or ACH instruction change. Call the bank or vendor back on a known number, never the number provided in the email or letter requesting the change. KEY
- Never let the same person both enter a bill and issue payment on it.
- Personally review and sign every check, or personally approve every electronic payment above a set threshold — no rubber stamps and no pre-signed checks.
- Require itemized, original receipts for all reimbursements and company credit card purchases.
- Periodically pull canceled checks and cleared transactions directly from the bank's own portal and review payees/endorsements yourself — not through a report the bookkeeper generated.

- Have an outside CPA or bookkeeping firm perform an independent reconciliation or review at least quarterly, even if you have in-house bookkeeping. For a business too small to separate duties internally, this is the single highest-value control available. KEY
- Conduct unannounced petty cash counts.

C. Payroll Controls

Payroll fraud is often invisible until a tax notice arrives — and by then, months or years of exposure may already exist.

- Personally review and approve the payroll register before it runs, every single cycle — not just the total, but who's on it and what they're being paid. KEY
- Segregate who can add or edit employees in the payroll system from who approves and releases the payroll run.
- Compare each payroll register to the prior period and investigate any unexplained changes in headcount, pay rate, or hours.
- Verify any direct deposit account change directly with the employee by phone or in person — never through email alone. A classic fraud pattern is redirecting a real (or recently terminated) employee's direct deposit to the fraudster's own account. KEY
- Review payroll tax filings and payments directly through the IRS/state tax portal rather than relying solely on your bookkeeper's confirmation. Unpaid payroll taxes are one of the most common bookkeeper failure patterns — and owners can be held personally liable for unpaid trust fund taxes regardless of who was supposed to handle it. KEY
- Terminate system and payroll access immediately upon an employee's departure — don't let this lag administratively.

D. Accounts Receivable & Customer Payments

- Have someone other than the person who records payments open the mail or receive incoming checks.
- Use a lockbox at the bank for mailed customer payments where the volume justifies it.
- Reconcile customer payments received against actual bank deposits, not just against the accounts receivable ledger — the ledger only shows what was recorded, not what actually landed in the bank. KEY
- Age your receivables and personally review the aging report monthly, not just at year-end.
- Watch for "lapping" — misapplying one customer's payment to cover a shortage created by an earlier, undeposited payment. Spot-check payment postings against deposits periodically.
- Require dual sign-off on any customer credit, refund, or write-off above a set dollar threshold.

E. Accounts Payable & Vendor Management

Fake or manipulated vendors are one of the most common ways a trusted employee quietly diverts company money.

- Maintain a formal, written vendor list and require owner approval before any new vendor is added to the system.
- Compare new vendor addresses and bank account details against your own employee address and payroll file. A classic fraud is a fake vendor set up using an employee's own address or personal bank account. KEY
- Require a purchase order or owner approval before any invoice over a set dollar amount is paid.
- Separate the person who enters bills into the accounting system from the person who approves and releases payment on them. KEY
- Never allow the same person to both add/edit vendors in the system and issue payments to them.
- Personally cancel or stamp invoices "paid" at the time payment is issued, to prevent the same invoice from being submitted and paid twice.
- Periodically review vendor payments for duplicate invoice numbers or suspiciously repeated amounts.
- Require supporting documentation (contract, purchase order, or delivery/receiving confirmation) before any payment is released.
- Periodically call or verify directly with a sample of vendors to confirm amounts owed and the account/payment details on file.
- Watch for round-dollar, sequential, or suspiciously regular invoice amounts from the same vendor over time — real invoices are rarely that tidy.

Online Vendor Accounts (Amazon, Walmart Business, etc.) & Purchasing Cards

This is one of the fastest-growing internal fraud patterns right now, precisely because it hides in plain sight: a purchasing agent with sole control over a company Amazon, Walmart Business, or purchasing-card account can order personal items and bury them in a stream of legitimate-looking purchases.

A real case that shows exactly why "asking questions" isn't enough on its own:

An administrative assistant at a Connecticut school district was the sole person with access to the district's Amazon account. Over five years, she purchased roughly 878 items totaling more than $40,000 — including a laptop, an iPad, a Nintendo Switch bundle, clothing, jewelry, and exercise equipment — all charged to the district. Her own statement to investigators confirmed that supervisors regularly did question her about the purchases. Each time, she justified them as materials needed for special education students or staff, and each time, the explanation was accepted. The purchases only stopped when a school resource officer independently pulled the actual Amazon order history rather than relying on her account of what had been bought.

Similar patterns show up constantly: a Tennessee city purchasing agent indicted for using a municipal Amazon account for personal purchases; a Florida medical practice employee convicted of grand theft after making more than 3,000 personal purchases on a company card; Kentucky employees charged with felony embezzlement for $18,000+ in unauthorized personal purchases on company cards. In every case, the same structural gap: one person could both place the order and explain it away.

- Separate who places online vendor orders from who has authority to approve or close out that spending. The person ordering supplies should never be the same person who reconciles or signs off on the account statement. KEY
- Require two independent approvers on purchasing card statements and online vendor accounts above a set monthly threshold — not one supervisor's sign-off, and no exceptions for someone who “always has a good explanation.” KEY
- Review the actual itemized order history on company Amazon/online vendor accounts monthly — not just the dollar total. A summary total will never show that a “supplies” charge was actually shoes, jewelry, or a game console; only the line-item detail will. KEY
- Use a shared company account with multiple authorized viewers for online vendor purchasing (e.g., Amazon Business with multi-user visibility) rather than a single employee's personal login tied to the company payment method.
- Apply merchant category code (MCC) restrictions on purchasing cards to block or flag non-business categories — personal care, apparel, electronics, entertainment — at the transaction level, before the purchase even completes.
- Set a hard rule that whoever has to justify an unusual purchase is never the same person with final authority to approve or close it out.
- Match itemized receipts or packing slips to an actual department, project, or budget line — a vague “supplies” description on an expense report should not be accepted on its own.
- Periodically have someone outside the purchasing function pull the full order history directly from the vendor's own portal, independent of any report or explanation the purchasing agent provides. KEY
- Ensure whoever audits or reviews purchasing card activity does not themselves hold a purchasing card — a reviewer auditing their own spending has no real oversight value.

F. Inventory & Fixed Assets

- Conduct a physical inventory count at least annually, ideally performed or verified by someone independent of day-to-day inventory recordkeeping.

- Maintain a tagged, numbered list of fixed assets (equipment, tools, technology) and reconcile it periodically.
- Lock and limit access to inventory and supply storage areas.
- Reconcile physical counts to the general ledger and investigate any variance, however small it may seem.
- Install cameras or alarm systems anywhere cash or high-value inventory is kept.
- Require documentation and a second signature for any inventory write-off or disposal.

G. The Bookkeeper's Seat: Segregation of Duties When One Person Wears Every Hat

This is the core issue behind most small business fraud, and it deserves its own section rather than a single bullet point.

In many small businesses, one bookkeeper can enter a bill, cut the check, sign it (or use the signature stamp), reconcile the bank statement, and record the general ledger entry — which means the same person positioned to commit a mistake or a fraud is also the person positioned to hide it. This isn't a character flaw in bookkeepers generally. It's a structural gap that exists because most small businesses can't afford three separate accounting employees, and nobody designed the workflow with fraud in mind.

- If you cannot fully separate duties because of the size of your business, add an independent compensating control: the owner personally reviews the actual bank statement directly from the bank — not the bookkeeper's reconciliation report — every single month, without exception. KEY
- Give the owner sole login credentials to the bank's online portal, or at minimum, structure access so the bookkeeper has entry-level authority only, with the owner holding sole release/approval authority. KEY
- Require a second signer on all checks and wires above a set dollar threshold — with no informal exceptions for “just this once.” Exceptions are exactly where controls fail. KEY
- Have an outside CPA or bookkeeping firm perform an independent quarterly review, even with in-house bookkeeping in place. For a business too small to separate duties internally, this is the single highest-value control you can put in place — full stop. KEY
- If there are multiple bank accounts, rotate which one the bookkeeper reconciles versus which one the owner personally spot-checks.
- Never let the bookkeeper be the only person who knows the login credentials, the location of paper records, or the process for a given task. Build in redundancy so a single person leaving — or being dishonest — doesn't leave the owner blind.

H. Systems, Access & Technology

- Maintain a list of who has access to each financial system — banking, accounting software, payroll — and review it quarterly.
- Deactivate system access immediately upon an employee's termination.
- Use unique logins for every user, never a shared login, so any action can be traced back to a specific person.
- Enable two-factor authentication on banking and accounting software wherever it's offered.
- Back up financial data independently of the bookkeeper's own systems and devices.
- Maintain an audit trail or change log in your accounting software and periodically review it for unusual edits, deletions, or backdated entries.

I. Insurance & Risk Transfer

Insurance doesn't prevent a loss — but it can determine whether the business survives one financially.

- Carry a fidelity bond or employee dishonesty coverage. This is the single most direct insurance product for the exact risk this guide addresses, and many small businesses simply don't have it. KEY
- Review coverage limits against your actual cash flow and exposure — not a stale figure from years ago.
- Understand your policy's specific requirements for filing a claim; many require a police report and proof of loss within a defined time window after discovery.
- Maintain cyber and crime coverage if the business uses online banking, ACH, or wire transfers.
- Review all coverage annually as the business grows — limits that were adequate at startup rarely stay adequate.

J. Independent Verification

- Have the books reviewed or audited by an outside CPA firm at least annually, even if it isn't legally required for your business. KEY
- If the business is too small to separate duties internally, treat the outside review as your primary control — not an afterthought.
- Personally review financial statements every month. Don't just glance at the bottom line — ask questions about anything that looks unusual.

Trust your bookkeeper. But verify independently. The two aren't in conflict — in fact, a good bookkeeper welcomes the verification, because it protects them too.

The Bottom Line

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

It happens because there was no system to get around — just one trusted person, wearing every hat, with nobody checking the bank statement directly.

Internal controls cannot eliminate every risk. But they can make sure one bad decision, one unverified transaction, or one unsupervised moment doesn't turn into a loss the business can't recover from.

Self-Assessment Scorecard

Seventeen 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
We check references and run background checks before hiring anyone with financial access.	☐	☐	☐
Our bookkeeper/accounting staff are required to take real vacation time each year.	☐	☐	☐
The owner personally reviews the actual bank statement directly from the bank every month.	☐	☐	☐
Wire/ACH instruction changes require independent call-back verification before any transfer.	☐	☐	☐
The same person cannot both enter a bill and issue payment on it.	☐	☐	☐
The owner personally reviews and approves the payroll register every cycle.	☐	☐	☐
Direct deposit account changes are verified directly with the employee, not by email alone.	☐	☐	☐
We reconcile customer payments received against actual bank deposits, not just the AR ledger.	☐	☐	☐
New vendors are approved by the owner, and vendor bank details are checked against employee records.	☐	☐	☐
Purchasing/ordering duties are separated from approval duties, with itemized (not just total) review of online vendor and purchasing card activity monthly.	☐	☐	☐
We conduct a physical inventory or fixed asset count at least annually.	☐	☐	☐
The owner — not the bookkeeper — holds sole release/approval authority on the bank's online portal.	☐	☐	☐
A second signer is required on all checks/wires above a set threshold, with no informal exceptions.	☐	☐	☐
System access is reviewed quarterly, and terminated employees are deactivated immediately.	☐	☐	☐
We carry a fidelity bond or employee dishonesty insurance policy.	☐	☐	☐
An outside CPA or bookkeeping firm reviews our books independently at least annually.	☐	☐	☐
The owner reviews full financial statements monthly and asks questions about anything unusual.	☐	☐	☐

30–34 points	**18–29 points**	**Below 18**
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 business should start.

Want to Talk Through Where Your Business Stands?

Summit Business Solutions works with owners across every industry on fractional CFO support, bookkeeping, and internal control reviews built around exactly this framework.

Travis Hawk, MBA — Summit Business Solutions LLC

405-850-4776 · travis@travishawk.com · travishawk.com