ThirdLine

10 Internal Control Checks Every Government CFO Should Run Monthly

A Comprehensive Guide for CFO's, Finance Teams, & Administrative Leadership

by ThirdLine

Introduction

Every month, Chief Financial Officers (CFOs) in local governments and school districts should perform key detective control checks to keep finances on track and safeguard against fraud. Proactive monthly oversight helps catch issues early before they grow into major problems. This is especially critical in the public sector, where fraud cases can cost a median of $150,000 each and even small municipalities have suffered devastating losses due to weak controls.

> As highlighted in a recent article from American City & County, "Without safeguards in place, fraud becomes easier to commit, and harder to catch."

This ThirdLine guide outlines ten essential detective controls for CFOs and their teams to conduct monthly. These steps, aligned with best practices and ThirdLine's continuous monitoring approach, will help detect fraud, reduce waste, ensure compliance, improve overall financial oversight, and make the year-end reporting much smoother.

Table of Contents

Who This Guide Is For

Finance and Accounting Teams: Responsible for ensuring accurate financial data and preventing fraud or mismanagement.

ERP Administrators: Tasked with configuring Tyler Munis, maintaining user accounts, and ensuring overall system integrity.

Compliance Officers: Concerned with audit readiness, policy enforcement, and compliance.

Department Directors and Managers: Responsible for transparency into what their teams can access, to mitigate risk and maintain accountability.

What is Internal Control?

Internal control refers to the system of policies, procedures, and practices that organizations use to safeguard assets, ensure accurate financial reporting, promote operational efficiency, and maintain compliance with laws and regulations. These controls help detect and prevent fraud, errors, and misuse of public funds. In essence, internal control is how an organization makes sure it does what it says it's going to do—safely, reliably, and responsibly.

The concept gained prominence in the mid-20th century, but it was the 1977 Foreign Corrupt Practices Act (FCPA) and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) that standardized the framework most used today. COSO's Internal Control—Integrated Framework (1992, updated in 2013) defined five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. Public sector agencies have adapted these principles to their own financial and operational landscapes, often under added scrutiny from elected officials, auditors, and the public.

What Are Preventive Controls?

Preventive controls are designed to stop errors, fraud, or irregularities before they happen. These proactive measures include segregation of duties, approval workflows, access restrictions, and policies that ensure transactions are authorized and reviewed prior to execution.

What Are Detective Controls?

Detective controls identify issues after they occur, allowing for timely investigation and correction. Examples include reconciliations, variance reports, audit trail analysis, and monitoring dashboards that surface anomalies or unauthorized activity.

What Are Corrective Controls?

Corrective controls are implemented to resolve problems uncovered by detective controls and prevent recurrence. These may include process redesigns, updated policies, disciplinary action, or system configuration changes based on audit findings.

The Principles of Internal Control Include:

1. **Control Environment:** The culture and tone set by leadership that promotes integrity, ethical values, and accountability.
2. **Risk Assessment:** Identifying and analyzing risks that could prevent the organization from meeting its objectives.
3. **Control Activities:** Policies and procedures put in place to mitigate risks and ensure directives are carried out (e.g., approvals, authorizations, reconciliations).
4. **Information and Communication:** Ensuring relevant information is captured and communicated timely and effectively across the organization.
5. **Monitoring Activities:** Ongoing evaluations to ensure that internal controls are present and functioning as intended, with issues identified and addressed promptly.

Internal controls are not just a nice-to-have compliance tool—they're a foundation of good governance. For CFOs, understanding and strengthening internal controls is critical for preventing fraud, maintaining trust, and ensuring accountability.

This guide will focus on Detective Controls, but we have other 10 step guides that focus on Preventive Controls.

Why You Should Care

Internal control failures are often invisible—until they're not. Fraud, compliance violations, and financial misstatements rarely begin as large, obvious events. They start small: a terminated employee left with ERP access, a vendor payment pushed through without review, a purchasing card used improperly. When these signals go unchecked for months or years, the consequences can be severe.

Municipalities and special districts have lost hundreds of thousands of dollars due to fraud schemes that went unnoticed for years. A 2024 report from American City & County showed that smaller governments—especially those with lean finance teams—are especially vulnerable to fraud due to gaps in monitoring, outdated systems, and under-resourced internal audit functions. In one high-profile case, a finance manager in a small town stole over $1 million by exploiting lax oversight in payroll and vendor payments.

By implementing a monthly cadence of control checks, CFOs gain the visibility and assurance needed to prevent those stories from repeating. These checks act as a force multiplier for financial oversight—bridging the gap between annual audits and day-to-day operations. They

empower finance leaders to detect irregularities early, ensure compliance with procurement and spending policies, and continuously reinforce trust with their boards, councils, and constituents.

Best of all, these checks can be automated.

You should care because of:

1. Fraud Prevention

Spot and stop internal fraud, vendor scams, and misuse before it escalates.

2. Operational Efficiency

Avoid the year-end scramble by resolving issues steadily throughout the year.

3. Governance & Accountability

Demonstrate strong financial stewardship to auditors, boards, and the public.

4. Cash Integrity

Ensure funds are spent as intended and avoid duplicate or unauthorized payments.

5. COSO Compliance

Regular monitoring aligns with the COSO framework to ensure internal controls stay effective and deficiencies are identified and addressed promptly.

“For departments to actively monitor and see breakdowns, ThirdLine provides more visibility to the data and helps management be better at defending the system.” Terence Williams, City Auditor, City of Wilmington, DE

The 10 Detective Internal Control Checks you can Automate

The following 10 checks are not just accounting best practices—they are strategic leadership tools. Done monthly, they position your finance team to stay one step ahead of fraud, reduce waste, and elevate accountability across your organization.

Additionaly, for each of these steps, we have Preventive Control Guides to fix the root cause problem.

Step 1: Analyze Payroll for Fraud, Errors, & Overtime

Why it matters: Payroll is often one of the largest expenses, and thus a prime area for potential fraud or mistakes. Each month, perform analytics on payroll data to spot anomalies. For example, look for ghost employees – ensure no one is getting paid after their termination date and that all listed employees are legitimate. Check for duplicate direct deposit accounts or Social Security Numbers across employees, which could indicate the same person being paid twice under aliases. Compare payroll deductions and tax withholdings among employees in similar roles; abnormally low deductions or taxes could signal manipulation or misclassification. Monitor overtime and special payouts: flag employees with unusually high overtime or those who received large one-time payouts like unused leave redemptions. Sudden year-over-year salary jumps without clear justification can also be a red flag.

1. Overtime and Leave Analytics: Review overtime hours and leave payouts. Excessive overtime that significantly inflates pay may indicate timecard fraud or abuse. Ensure leave payouts or buyouts are properly approved to catch any unauthorized self-payments (as seen in past fraud cases).
2. Ghost & Duplicate Checks: Run a report for any payments made to employees who have separated (after termination date). Also, scan for multiple employees sharing the same bank account or SSN, which is a major red flag for payroll fraud.
3. Compare Deductions/Withholdings: Use analytics to spot any employees with unusually low tax or benefit deductions compared to peers. This could uncover cases where someone illicitly reduced their withholdings or benefit contributions.

These payroll checks help deter insider fraud like fake employees or inflated pay. In one notorious case, a small-town finance officer gave herself unauthorized raises and never recorded her time off, stealing over $1.1 million via payroll over 19 years. Regular analytics can catch such patterns early, safeguarding public funds and employee trust.

Step 2: Review Changes to the Vendor Master Records

Why it matters: A clean vendor master file is crucial for preventing fraud and ensuring efficient procurement. Each month, review the vendor master data for changes.

1. Purge Duplicates: Identify any duplicate vendor names or EIN/Tax IDs in the system. Merge or eliminate duplicates to prevent double payments and confusion.

2. Put Stale Vendors on Stop Status: Create a policy to put Vendors on "STOP" status that have not been paid in years, or who don't have an active P.O.
3. Update Required Documents: Confirm that new vendors have provided necessary forms (W-9, insurance, licenses) and that existing vendor records are refreshed with any new compliance info each month. This ensures enhanced compliance and accuracy in your payables.

Procurement Director Case Study – Cleaning up the Vendor Master:

An up-to-date vendor master reduces both fraud risk and inefficiency. When ThirdLine helped one city clean its vendor data, the Procurement Director noted it “saved us 2.5 weeks of work” and freed staff to focus on more strategic tasks by automating vendor list management. A cleaner vendor file means staff spend less time fixing data issues and more time on value-added activities.

Step 3: Review Changes to User Access and Permission

Why it matters: Ensure that employee access to financial systems remains tightly controlled. Each month, audit all active ERP users and their role permissions for appropriateness and signs of “permission creep.” Remove or deactivate any users who have left the organization or no longer need access, and turn off roles that have no active users. Pay special attention to powerful default roles (like the broad “MUNIS” admin role) and restrict them to only those who truly require such access. Also, check for segregation of duties (SoD) conflicts in user roles – no single person should control incompatible tasks (e.g. creating and approving transactions) as this poses a fraud risk. By keeping roles and privileges up to date, you prevent internal fraud and errors, maintain compliance by reducing SoD violations, and eliminate unnecessary access that could be exploited.

1. Review Terminated Employees and those who Switched Positions: Immediately revoke access for terminated or inactive users and ensure employees who switched positions or departments have old ERP Roles removed
2. Enforce Least Privilege: Regularly review who has high-level permissions (such as system admin rights) and ensure their access aligns with current job duties. Remove excessive privileges to minimize security gaps.

3. Check SoD Conflicts: Use reports or analytics to flag users with conflicting roles or excessive capabilities (e.g. a user who can both initiate and approve payments). Restructure duties or adjust roles to resolve these conflicts and strengthen oversight.

We highly recommend a full review of your Roles, Permissions, and Business Rules as a Preventive Control.

Step 4: Audit Purchasing Card (P-Card) Transactions

Why it matters: Purchasing cards (P-cards) and employee credit cards streamline small purchases but come with fraud and misuse risks. Each month, perform an audit of P-card usage. Review all card transactions for compliance with your p-card policies (appropriate merchants, spending limits, no personal expenses, etc.). Analytics can greatly aid this review: for instance, flag any instances of split transactions on P-cards, where a cardholder has multiple swipes at the same vendor on the same day that together exceed the single-purchase limit – a tactic sometimes used to evade spending caps. Also conduct a keyword search on transaction descriptions for any suspicious terms (your policy might forbid certain items or require notation of business purpose – keywords like “gift”, “cash”, or missing descriptions could warrant a closer look).

Another useful check is monitoring approval patterns: if one supervisor is approving an unusually high volume of transactions daily, ensure they are really reviewing them or if perhaps rubber-stamping is occurring due to workload. Verify that card limits for each employee are still appropriate given their spending patterns; adjust limits or revoke cards if usage is consistently low or if there are concerns. Crucially, ensure there is documentation (receipts) and authorization for each transaction as per policy.

1. Split Purchase Detection: Look at transactions by department or cardholder to catch multiple charges that should have been a single larger purchase requiring a PO. For example, 5 purchases of $900 to the same vendor in one month might violate a $2,500 single-purchase bid limit and indicate policy evasion.
2. Unusual Merchant or Item Review: Scan for any purchases at merchants that are not typical for business needs or allowed categories (e.g. liquor stores, high-end electronics, etc.). Also flag transactions made on weekends or holidays, which might be personal in nature.
3. Limits and Approvals: Ensure each transaction was approved by the assigned reviewer. If an approver has dozens of transactions to approve in a short period, consider if the workload is too high to give proper scrutiny. Additionally, periodically re-

evaluate cardholder spending limits – they should be high enough to cover business needs but low enough to mitigate risk.

Monthly P-Card audits help detect fraud, waste, or misuse quickly, allowing the organization to take corrective action (discipline, require reimbursement for personal charges, retraining on policies) without waiting for an annual audit. They also reinforce to employees that card use is being watched, which is a powerful deterrent against inappropriate spending. By using analytics and continuous monitoring, one city was able to automatically identify high-risk P-card transactions and even optimize card limits based on spending trends. The result is a p-card program that is convenient and controlled – empowering employees to do their jobs while protecting the organization from abuse.

Step 5: Identify Duplicate Payments and Invoice Errors

Why it matters: Duplicate vendor payments are a common and costly error in accounts payable. Each month, CFOs should run an audit for duplicate invoices or payments to vendors. This involves checking for any invoices with the same vendor, invoice number, and amount that may have been paid twice, as well as any vendor that was paid the same amount on the same date (potential indicator of a duplicate). Causes of duplicate payments include data entry mistakes, duplicate vendor records, or vendors accidentally submitting an invoice twice. Even if accidental, these overpayments drain funds and often go unnoticed without a deliberate check. Catching them monthly means you can recover the funds quickly and correct the process to prevent future occurrences.

1. Same Same Difference Tests: Use an analytic to scan the AP ledger for identical invoice references (number, date, amount). Also look for invoices that are very similar (amounts within a few cents or same date and vendor) which might be duplicates entered slightly differently.
2. Review Credit Memos/Adjustments: Sometimes duplicates are caught by staff and a credit memo is issued by the vendor. Track such credits and ensure they are actually received or applied. If you find a duplicate that wasn't resolved, contact the vendor promptly for a refund or credit.

3. Duplicate Vendor Cleanup: As noted in step 2, duplicate vendor records can lead to paying the same entity twice. Ensure you audit vendors with similar names, addresses, EIN's or emails. Merging those records will reduce the risk of duplicate payments.

Virginia Beach Case Study – Recovering Duplicate Payments: Even well-run cities can lose money to duplicate vendor payments. In Virginia Beach, a contingency audit using ThirdLine's analytics uncovered more than $40,000 in duplicate payments that had slipped through over time. The city was able to recover these funds, directly boosting the budget, and implemented continuous monitoring to flag any future duplicates in real-time. This example underscores how a simple monthly duplicate check can save money and strengthen controls, turning up immediate recoveries and preventing costly mistakes from lingering.

Detecting and eliminating duplicate payments provides an instant ROI – in many cases, recovered money that goes straight back to your bottom line. It also improves vendor relationships (by avoiding the awkwardness of asking for refunds months late) and demonstrates strong financial control to auditors and the public. A robust process, possibly automated with tools, to catch duplicate invoices ensures that no dollar is paid more than once, reinforcing the stewardship of public funds.

Step 6: Monitor for Fraud Signals through Vendor Payment Activity

Why it matters: Vendor fraud – especially schemes where criminals impersonate legitimate vendors to reroute payments – is on the rise and can lead to huge losses if undetected. Additionally, employees can commit fraud buy creating and paying illegitimate companies. To guard against this, implement a monthly (if not more frequent) review of any changes in vendor master data and certain payment patterns. CFOs should receive a report of all vendor account changes made (bank account updates, mailing address changes, new vendor entries, etc.) and spot-check those for validity. Key changes to watch include: a vendor's bank account or routing number change, a switch in payment method (e.g. from check to ACH or vice versa), or an address/email change – especially if followed shortly by a large payment request. Such scenarios could indicate someone inside or outside attempted to divert funds. It's wise to verify significant changes directly with the vendor using known contact information on file (not the potentially fraudulent new info).

1. Vendor Change Log Audit: Review the log of changes in vendor records. For each banking detail change, confirm that a proper verification was done. This might involve calling the vendor's known phone number to confirm they requested the change – a

simple but effective anti-fraud control.

2. First-Payment After Vendor Master Change: Have a policy to thoroughly review the first payment made to any new vendor, especially if that payment is above a certain threshold. Combine data from AP and vendor master to flag if a normally dormant vendor suddenly has activity. Verify the supporting documents and that the new vendor information is legitimate (e.g. look up their business registration). Many organizations catch fraud when a phony vendor's first invoice is flagged before payment.
3. Vendor & Employee Master Record Matching: Internal Fraudsters (Employees) are surprisingly not that sophistacated in how they commit fraud. By simply matching key fields between the Vendor Master and Employee Master, you can catch fraud. Key fields like bank account numbers, phone numbers, emails, and addresses can reveal a fraud scheme

By diligently tracking vendor info changes and payment anomalies, CFOs can stop vendor fraud attempts in their tracks. In the event something does slip by, an early detection can still facilitate recovery. Remember that without monitoring, a fraudulent vendor diversion might go unnoticed until the legitimate vendor complains about missing funds – by then the thief is long gone. A monthly vendor fraud check, ideally as part of a continuous monitoring system, gives you the upper hand. It provides real-time fraud detection and alerts, enhancing financial security by ensuring payments only go to authorized, verified accounts. This level of vigilance also keeps your organization in compliance with internal control policies and audit requirements, demonstrating that you are actively safeguarding public assets.

Step 7: Review Requisitions and Invoices in Approvals and Workflows

Why it matters: Inefficient approval workflows can both delay operations, create cash flow uncertainty, inaccurate financial reports, and weaken controls. Each month, the CFO should review any pending or stuck approvals in the financial system – for purchase orders, vendor invoices, expense reports, etc. Identify items that have been sitting in someone's queue or awaiting approval longer than the acceptable threshold (e.g. >30 days). Often, invoices and requisitions get stuck in limbo due to bottlenecks, contributing to slow month-end closes. By monitoring these, you can prod managers to take action or re-route approvals as needed. Also look for any instances of approval overrides or bypasses – transactions forced through without proper sign-off – and investigate those for policy compliance. Maintaining real-time visibility into the approval process ensures nothing slips through unchecked or causes undue delay and inaccurate financial reports.

1. Aging Approval Report: Generate a list of all requisitions, POs, and invoices pending approval and their age. Focus on clearing old items to keep the process flowing and avoid piling up unrecorded liabilities at month-end.
2. Identify Bottlenecks: Note if certain departments or approvers consistently cause delays. For example, if a particular manager has many items pending, ensure they have support or escalation. Use data to foster accountability rather than relying on blame games.
3. Enforce Approval Controls: Check that all expenditures went through the proper workflow. If any payments were processed with missing approvals or outside the normal process, flag them for immediate review as they indicate a breakdown in the set-up of Business Rules.

Regularly clearing approval backlogs not only accelerates the monthly close but also strengthens financial oversight. It prevents scenarios where invoices are paid late or without review and budget to actuals are accurate. With the help of workflow dashboards, some organizations achieve faster invoice approvals and improved accountability by highlighting where approvals stall. Keeping the approval pipeline clean each month means your organization can close the books on time and confidently, with all transactions properly authorized.

Step 8: Review Budget vs. Actual Variances

Why it matters: A monthly budget-to-actual review is a cornerstone of financial oversight. The CFO and finance team should analyze any significant variances between budgeted and actual figures for the month and year-to-date. Consider how stuck Requisitions in Step 7 need to be included in this analysis. Focus on areas with substantial overspending (actual > budget) or underspending (actual < budget) beyond a set threshold (e.g. ±10%).

Large variances can signal errors (mis-coded expenses), emergent needs, or lack of spending control. Unresolved variances can raise red flags during audits, leading to penalties or reputational damage if not explained. On the flip side, chronic underspending might mean missed opportunities – for example, unspent grant funds that end up forfeited. Investigate the root causes: was there unexpected activity, or were assumptions off? Require department heads to provide explanations for big variances and action plans (such as budget transfers, spending cuts, or additional funding requests) as needed.

1. Automated Threshold Alerts: Leverage your ERP or analytics tools to trigger alerts for any expenditures that exceed budget by a certain percent or amount. This helps catch issues in real-time rather than weeks after.

2. Drill Down by Department/Project: Examine variances at a granular level – which department or program is driving the variance? Use dashboards to pinpoint the specific area and line items causing the deviation. This targeted approach makes it easier to find and fix problems (e.g. a project overspending on overtime).
3. Document Explanations: For each major variance, record the explanation and any follow-up actions. This creates a trail of accountability and a knowledge base for future budgeting. Patterns of variance can inform adjustments to forecasts or controls (for example, if one department consistently overspends on a certain expense, perhaps the budget was unrealistic or controls need tightening).

By performing variance analysis monthly, CFOs improve fiscal responsibility through early detection of budget issues. It enables proactive adjustments – reallocating funds or tightening controls – before small variances escalate into big deficits. It also supports transparency: stakeholders see that management is actively monitoring finances and addressing exceptions, which enhances their confidence in financial governance.

Step 9: Review Non-Standard Journal Entries

Why it matters: Manual journal entries are one of the highest-risk activities in the financial close process. Each month, CFOs should use analytics to test journal entry data for anomalies that could indicate errors, misstatements, or fraud. Focus on entries posted outside business hours, those with large round numbers, missing documentation, or unusual account combinations.

Using filters or queries in your ERP or analytics platform, identify:

1. Entries posted manually outside working hours, on the weekend, or on a holiday
2. Journal entries posted to suspense or high-risk accounts
3. Transactions posted by users without appropriate role clearance
4. Manual Journal Entries that were not posted in the same period in the previous year
5. Manual Journal Entries that could be duplicates by reviewing those with the same dollar amount and account classification

Each flagged entry should be reviewed for adequate backup, explanation, and appropriate authorization. Journal entry testing is a detective control that can uncover not only mistakes, but deliberate attempts to manipulate financial statements. Embedding this step monthly increases accountability and strengthens the integrity of your general ledger.

Step 10: Monitor Procurement Process & Contract Compliance

Why it matters: Procurement is an area rife with opportunities for cost savings as well as risks of waste or abuse. Each month, CFOs should review purchasing activity for adherence to policies and to spot any anomalies. Ensure that purchases are complying with procurement rules such as competitive bidding requirements, spending limits, and contract terms.

Leverage purchasing analytics to flag unusual transactions. Some examples include:

1. Duplicate Requisitions (e.g. two reqs with the same vendor, amount, and date – could indicate a duplicate entry or an attempt to game the system)
2. First-time vendors receiving large POs (warranting extra due diligence before payment)
3. P.O. Splits: Identify any instances of apparent split purchases – multiple smaller requisitions or POs that together exceed approval thresholds or bid limits, done intentionally to evade RFP's or competition. For example, if one or multiple departments made several purchases just under the bid limit from the same vendor within a short period, this should be flagged (this pattern is similarly detectable in P-Card usage).

By actively monitoring procurement, CFOs encourage efficient, compliant spending. Data-driven scrutiny of purchasing not only deters employees from bending rules, but also can highlight opportunities to save money (for instance, consolidating duplicate requisitions, catching when a lower-cost vendor could be used, etc.). Healthy purchasing controls promote competition and fairness in supplier selection, benefiting the organization's reputation with vendors and the public. In summary, this monthly check helps ensure you procure goods and services at the best value and according to the rules – a critical aspect of fiscal stewardship.

Call to Action: Embrace Continuous Monitoring & Auditing for Detective Controls

Performing these 10 detective control checks monthly will significantly strengthen your organization's financial oversight and integrity. They are an antidote to the complacency that fraud relies on.

The key is to make these activities part of a continuous monitoring strategy rather than one-off annual checkups. Continuous auditing and monitoring uses automated tools and data analytics to test 100% of transactions in near real-time, providing early warnings of issues. It leads to swift detection of errors or fraud, increased efficiency through automation, improved compliance, and proactive decision-making based on actionable insights.

ThirdLine: Modern Software to Audit, Report, and Optimize your ERP

ThirdLine's analytics platform is purpose-built to help finance teams implement these monthly control checks—seamlessly aligned with the five principles of internal control:

1. We help establish a strong control environment through transparent reporting and role clarity.
2. Our risk-based dashboards support proactive risk assessment across ERP functions.
3. Policies tied to analytics ensures high-integrity control activities.
4. Tailored alerts and department-level reporting enhance information and communication.
5. And real-time dashboards and exception monitoring drive continuous monitoring activities.

By aligning with the COSO framework, ThirdLine helps government CFOs strengthen their control posture, reduce exposure, and create a lasting culture of accountability.

Call to Action: Commit to implementing these monthly financial control checks in your organization. If you already do some of them, evaluate how to enhance them. If you want help, reach out to ThirdLine. If some are new, develop a plan to phase them in. By moving toward a culture of continuous auditing and improvement, CFOs can ensure that they protect public funds, uphold transparency, and stay one step ahead of fraud.