AUDIT & BEYOND | IN-PERSON OR VIRTUAL | OCTOBER 21-23, 2025 REGISTER NOW

August 5, 2025 • 24 min read

Internal controls to prevent fraud: A practical guide

Brandi Anastasiades

ON THIS PAGE

Organizations worldwide lose an estimated 5% of revenue to fraud annually, with total analyzed losses exceeding $3.1 billion. In fact, more than half of occupational frauds occur **due to a lack of internal controls** or an override of existing internal controls. Most organizations are playing defense with outdated playbooks where they don't implement internal controls or don't do it the right way.

So here's the million-dollar question (literally, since the average fraud case costs organizations $1.7 million): **How do you build a defense system that actually works?** How do you create internal controls that don't just look good on paper but genuinely prevent fraud before it happens?

In this guide, we'll walk you through the specific internal controls that prevent the most common types of fraud and how you can avoid the pitfalls that leave so many organizations vulnerable.

What are internal controls, and why do they matter for fraud prevention?

Internal controls are the **policies, procedures, and mechanisms** designed to ensure accurate financial reporting, promote operational efficiency, and prevent fraud. For fraud prevention, they serve three critical functions:

- They make fraud harder to commit.
- They're more likely to detect fraud quickly.

COOKIE SETTINGS

- They're easier to investigate when fraud does occur.

Think of internal controls as the organizational equivalent of a home security system. Relying on a single control is like securing your network perimeter but leaving endpoints unprotected — layered, complementary controls are essential to reducing, preventing, and detecting fraud risk. The median loss from fraud is $60,000 when committed by employees and $500,000 when committed by owners or executives, according to the ACFE. **The longer it takes to detect fraud, the higher the losses.**

The most effective internal controls operate on the principle of making fraud inconvenient and risky for potential perpetrators. When someone has to work harder, involve more people, and leave more evidence to commit fraud, most simply won't bother.

That's why you need to focus on detection *and* prevention to prevent fraud in the long run.

Who's responsible for implementing and monitoring internal controls?

To establish an effective internal control fraud prevention program, it is integral to have clearly defined responsibilities across your risk management program. Here's what that looks like:

- **Leadership sets the foundation:** The C-suite and senior leadership team are responsible for establishing the organization's risk appetite and creating a culture that doesn't tolerate fraud. Based on these aspects, they can help you allocate adequate resources to fraud prevention.
- **Process owners manage execution:** The people executing day-to-day business process activities (e.g., risk prevention programs, accounts payable, vendor relationship management, payroll, cash receipt handling, journal entries, etc.) are responsible for implementing and maintaining controls within their areas. They need to understand why the controls exist and how to spot when something isn't working properly.
- **GRC and compliance teams orchestrate and assess the framework:** GRC or compliance teams ensure controls are documented, that responsibilities are clearly defined, that control effectiveness is regularly assessed and that issues are promptly addressed. They're the connective tissue that makes sure everyone else is doing their part.
- **Internal audit owns the independent risk assessment:** Internal audit directors evaluate whether controls are designed effectively and operating as intended. They can conduct internal audits and tell leadership when controls aren't working, when gaps exist, or when management is taking unacceptable risks.

The most successful fraud prevention programs are those where everyone understands that controls exist to protect the organization — and their own jobs — from the devastating impact of fraud. So, establish clear escalation procedures for when controls fail or when someone tries to override them.

What kinds of internal controls exist to prevent fraud?

Here's a list of specific controls that stop the most common fraud schemes before they become a problem:

COOKIE SETTINGS

Segregation of duties

Segregation or separation of duties is your best friend when it comes to preventing fraud. The goal is to make sure one person can't execute *the entire* transaction on their own. When different people are given different duties to complete a single transaction, it's harder to commit a fraudulent one. It prevents fraud types like payroll fraud and procurement fraud.

In payroll fraud, this means separating the functions of adding new employees, entering time and pay rate changes, and approving payroll runs. But when it comes to procurement fraud, you want to separate requisitioning, purchasing, receiving, and payment approval functions.

Example: Your accounts payable clerk can enter vendor invoices but can't approve payments over $5,000. Your HR generalist can enter new employee data but can't approve salary changes. As a result, when someone thinks of committing fraud, they now need an accomplice, which makes it harder to commit fraud.

Periodic reconciliations

Reconciliations help you spot when something doesn't add up before minor discrepancies become real problems. They prevent fraud types like expense reimbursement fraud and financial statement fraud. Ideally, you should make sure it's performed by someone independent of the processes being reconciled.

Example: Your finance team reconciles bank statements monthly, but they also conduct analytical reviews comparing current-period expenses to those of prior periods and budgets. When they notice that an employee has filed a travel expense but there is no travel record or they're exceeding the budget more recently, it'll be considered an anomaly. So, your finance team will raise additional concerns to make sure it's a real expense.

Authorization workflows

Authorization workflows establish checkpoints that require proper business justification before employees can complete transactions. They're particularly effective against fraud schemes that rely on bypassing normal approval processes or creating fictitious transactions — such as in the case of procurement or financial statement fraud.

Example: Implement controls where purchase orders over $10,000 require department manager approval, over $50,000 require division director approval, and over $100,000 require C-level approval. You can also extend this policy to other processes, such as new vendor setups, payments to specific vendors, or access to specific records.

Whistleblower hotline programs

Whistleblower hotlines are meant to prevent illegal and unethical practices like bribery and corruption — but they're difficult to detect through traditional controls. According to the U.S. Securities and Exchange Commission (SEC), the most common fraud areas are:

COOKIE SETTINGS

- Manipulation (37%)
- Offering fraud (21%)
- Initial coin offerings and crypto-asset securities (8%)
- Corporate disclosures and financials (8%)

A good whistleblower program creates a culture where people feel safe reporting concerns and confident that their reports will be taken seriously. This means ensuring anonymity, prohibiting retaliation, and following up on all reports in a timely manner.

Example: If your hotline accepts reports via phone, the report must be managed by an independent third party or a legal department. Every report should be documented with a tracking number, allowing you to track its status and escalate it if needed.

Documentation and evidence standards

When you have strong documentation requirements, it makes it much harder for people to create false transactions or manipulate existing ones. Since everything has an audit trail and is reviewed by a third party, you can curb the problem right at the source.

Example: You can implement policies that require all journal entries exceeding $25,000 to include supporting documentation and obtain manager approval before posting.

3 real-world examples of internal controls preventing fraud

We can discuss internal controls in theory all day, but what really matters is how they perform (or fail) when put to the test in actual organizations. Here are three recent cases that show you why you need internal controls in the first place:

Morgan Stanley

In 2024, Morgan Stanley paid approximately $249 million in disgorgement and penalties to resolve SEC charges related to improper disclosure of confidential information about large stock sales. Both the firm and a senior executive were sharing confidential "block trade" information, giving some clients unfair advantages while trading in the market.

The company didn't have the right authorization workflows in place for handling sensitive information like confidential trading data. If it had implemented strict authorization workflows requiring multiple approvals for any disclosure of confidential trading information, this fraud would have been much harder to execute and easier to detect.

Macy's

A single Macy's employee managed to hide up to $154 million in falsified expenses by manipulating small-package delivery expense accounting. The fraud went undetected for years because Macy's didn't conciliations and independent oversight of expense accounts or failed to see the

COOKIE SETTINGS

pattern over the years. Ideally, if they had conducted regular analytical reviews comparing delivery expenses to sales volumes, it would have been much easier to identify the hidden expenses.

SEC's Whistleblower program

In 2024, the SEC issued $255 million in awards and received over 24,000 whistleblower tips — representing fraud and misconduct that was caught and stopped because employees had a safe mechanism to report concerns. In fact, J.P. Morgan had to pay one of the highest settlements ($18 million) for impeding employees from contacting the SEC. It goes to show that even with the right controls in place, if you don't have independent parties evaluating your controls, it can undermine the entire risk mitigation strategy.

What common weaknesses exist in fraud control programs?

There are many fraud control programs that look great on paper but don't hold up when somebody actually tests them. This happens when organizations don't account for weaknesses such as these:

1. Over-reliance on manual controls

Manual controls are only as reliable as the people operating them, and people tend to become busy and distracted over time. When your fraud prevention strategy relies on someone remembering to check, review, or approve something every single time, it won't be as effective as you need it to be.

The problem is that manual controls are easily bypassed when people are under pressure to get things done quickly. Time-sensitive exceptions are often used to bypass controls — like during an emergency or month-end cycles. That's why you should move toward automated enforcement mechanisms and escalation protocols wherever possible. For instance, instead of relying on someone to remember to review high-dollar transactions, build system controls that automatically route transactions over certain thresholds to the appropriate approver.

2. Lack of monitoring or follow-up

Organizations spend time and money designing elaborate control frameworks, documenting them beautifully, and training people extensively on them. But they forget to see if it's actually working.

When you design fraud prevention programs, make sure to include the following:

- Regular control testing
- Trend analysis of control failures
- Accountability measures for control owners
- Regular risk assessments to ensure control framework remains agile and aligned to the business

When people know that control performance is being measured and reported, they're much more likely to take them seriously.

COOKIE SETTINGS

3. Inconsistent documentation

The purpose of documentation is to support business needs and validate the end goal, such as a transaction or approval. That's why documentation requirements should be risk-based, consistently applied, and reviewed by someone who understands what they're looking for. In 2024, Inscribe found that in 48% of document fraud cases, first-party data (such as identity and financial information) was edited — making it harder to identify fraud.

So, create a **list of workflows within each department**, including the documents required for each approval and the individuals who will need to review and approve them. This will help you create an audit trail that makes it harder to commit fraud.

4. Limited awareness training

It's common for organizations to provide presentations about the importance of ethics, have employees sign acknowledgment forms, and then return to their jobs. However, they may not have measures in place to track whether employees can identify fraud or report it themselves. Phishing drills only *scratch the surface* of what's possible.

Effective fraud awareness training is tailored to specific roles and scenarios. Your accounts payable team needs to know what vendor fraud looks like and how to spot fictitious invoices. And your managers need to recognize the behavioral indicators that might suggest someone is under financial pressure or considering fraudulent activity. If they're trained appropriately and have the tools to help them identify suspicious activity, they can improve their ability to detect fraud over time.

How AuditBoard supports internal controls and prevents risk of fraud

You can design the most sophisticated fraud control framework in the world, but if you can't implement it efficiently, monitor it effectively, and improve it continuously, there's a chance your organization will remain vulnerable. Let's look at how AuditBoard helps you find your blind spots and mitigate risk effectively:

1. Automate internal control workflows with ease

AuditBoard's automated workflow capabilities change how organizations manage internal controls. Instead of relying on someone to remember to perform a control test, you can configure automated workflows that ensure controls are completed consistently, thoroughly, and on schedule.

Here's what it looks like in action: Control execution and self-assessment tasks are automatically assigned to the responsible team members with built-in escalation if they're not completed on time. The best part is that there's an audit trail for every action within the platform. As a result:

- Every control activity is logged, timestamped, and documented, creating an unbreakable chain of evidence.

COOKIE SETTINGS

- When someone tries to claim that they performed a control when it wasn't or when you need to investigate a control failure, you have complete visibility into what occurred.
- Nobody can alter or delete the data because it's logged and needs additional permissions to actually delete the data.

2. Track issues and anomalies in real time

The problem with traditional control monitoring is that by the time you identify an issue, it's often too late to prevent significant damage. With Auditboard, that's not the case. It has real-time monitoring capabilities to help you identify potential fraud indicators as they occur, not weeks or months later.

Here's what it looks like in action: If there are unusual transaction patterns, control failures, or other red flags, it triggers immediate alerts to the appropriate team members. The platform's analytics capabilities go beyond simple alerting to provide sophisticated pattern recognition that can identify potential fraud within your organization. Its machine-learning algorithms analyze transaction patterns, identify anomalies, and flag potential issues for human review.

This **doesn't replace human judgment** — it augments it by ensuring that potential problems don't get lost in the noise of day-to-day operations.

3. Access control testing dashboards for proactive monitoring

Managing preventive controls for fraud without comprehensive visibility makes it challenging to understand what is impacting your compliance outcomes. AuditBoard's dashboard gives you the visibility you need to understand control performance, identify trends, and make informed decisions about control improvements.

Here's what it looks like in action:

- You can see which anti-fraud controls are being performed consistently, which ones are experiencing frequent exceptions, and which ones might need attention.
- Instead of waiting for quarterly control assessments, you have continuous insight into how your fraud prevention program is performing.
- When you can see patterns across multiple controls, business units, and periods, you can identify systemic issues which aren't evident when you review metrics in isolation.
- You can also improve your risk management/mitigation or internal control strategy over time by using the data in this dashboard.

Plus, you can customize your dashboards depending on who's the audience for it — like leadership or your GRC/audit team.

COOKIE SETTINGS