Internal Controls Are Not Always Fraud Controls: Are You Looking for Intentional Deception?



ARTICLE 11.13.26 JODI RENN, CPA, CIA, CFE, CRMA

Fraud Awareness Week is a good time to take a step back and consider an important question: Are your internal controls designed to catch honest mistakes, or would they also identify someone intentionally trying to deceive you?

Most organizations have established internal controls. Invoices are approved, bank accounts are reconciled, expenses are documented, and system access is restricted. These controls are important, but they are not automatically fraud controls. They are typically designed to support accuracy, completeness, and compliance, and they work well when errors are accidental. Fraud is different because it involves intent. Someone committing fraud often understands how your processes work and may know exactly how to make a fraudulent transaction appear legitimate.

The Difference Is Intent

Consider a routine invoice approval. A manager confirms the supporting documentation is in place and approves the payment. That review may catch missing support, mathematical errors, incorrect coding, and amounts exceeding approval limits. But what happens when the invoice is fictitious and the supporting documentation has been created to look legitimate?

The control may have worked exactly as designed. The issue is that it was never intended to determine whether the information was authentic.

This distinction is important when evaluating whether existing controls are adequately addressing an organization's fraud risks. Following a process and identifying intentional deception are not necessarily the same thing.

Prevention Matters, but So Does Detection

No organization can prevent every attempt at fraud, which makes early detection critical. According to *Occupational Fraud 2026: A Report to the Nations*, the typical fraud in the study continued for 12 months before it was detected. Frauds identified within six months had a median loss of $40,000, compared with $100,000 for those lasting seven to twelve months.

Organizations may not be able to stop every attempt, but they can take steps to make fraud harder to commit, harder to conceal, and more likely to be identified quickly.

This requires looking beyond whether established procedures are being followed and considering whether monitoring activities can identify unusual patterns, inconsistencies, and exceptions.

Three Questions to Ask About Your Higher-Risk Processes

Strengthening fraud controls does not necessarily require additional approval layers or sophisticated technology. A practical starting point is to select a few higher-risk processes and consider whether existing controls address the ways fraud could actually occur.

1. What are we trying to prevent?

Start with the potential fraud risk rather than a list of existing controls. In accounts payable, for example, could someone create a fictitious vendor, submit an altered invoice, change vendor banking information, generate duplicate payments, or structure transactions just below approval thresholds?

Consider which controls would specifically address those scenarios. An organization may have a well-established approval process, but does that process actually address the possibility of intentional manipulation?

2. How would we detect it?

Look across transactions rather than focusing only on whether each individual transaction was approved. Patterns worth watching include:

- Payments that repeatedly fall just below approval thresholds.
- Frequent changes to vendor banking information.
- Vendors that share addresses or accounts.
- Unexplained overrides, manual transactions, or activity involving dormant vendors.

Many organizations already have access to the data needed to identify these patterns. The opportunity is often in how that information is reviewed and analyzed.

The 2026 report found that organizations using proactive data monitoring and analysis had a median fraud loss of $70,000, compared with $150,000 for those without it.

3. How could someone get around the control?

Consider whether supporting documents could be altered, whether the reviewer independently verifies critical information, whether two people working together could circumvent the control, and whether overrides receive meaningful review.

It is also important to consider what happens if a key fraud control stops operating. Would anyone recognize that it was no longer being performed?

Evaluating controls from this perspective helps organizations identify potential weaknesses that may not be apparent when simply confirming that established procedures are being followed.

Sometimes the Best Fraud Control Is a Focused Review

Organizations may not need another approval step or checklist to strengthen their fraud controls. Sometimes, a more focused review that asks a specific question can be more effective.

For example, instead of only asking, “Were all vendor changes properly approved?” consider asking, “Which vendors changed banking information this quarter, who approved each change, how was it independently verified, and were payments redirected afterward?”

The first question confirms that the process was followed. The second looks more closely at whether fraud could have occurred.

The same approach can be applied to payroll, purchasing, expense reimbursement, corporate credit cards, journal entries, inventory, and system access.

The objective is not to add unnecessary complexity, but to ensure that reviews are addressing the risks that matter most.

Don’t Overlook the Human Side

Analytics are only part of the picture. According to the 2026 report, 43% of occupational fraud cases were first detected through tips, nearly three times the rate of the next most common detection method.

This reinforces the importance of an organization’s culture and reporting environment. Employees and other stakeholders may recognize unusual activity long before it appears in a financial report or management review.

Organizations need monitoring processes that flag unusual activity, along with a culture and reporting process that encourages people to raise concerns when something doesn’t seem right.

Technology can help identify patterns, but people often provide the context needed to recognize potential misconduct. Both play an important role in an effective fraud risk strategy.

A Different Question for Fraud Awareness Week

Instead of asking, “Do we have adequate internal controls?” consider asking, “Which of our controls are specifically designed to address intentional deception, and how quickly would we know if someone found a way around them?”

The answer may be that your organization does not need more controls, but rather a different way of evaluating the ones already in place.

Taking the time to look at existing processes from a fraud perspective can help organizations identify potential gaps, better understand their exposure, and determine where additional attention may be needed.

Let’s Take a Look at Your Controls Together

Dean Dorton’s fractional internal audit professionals can help organizations evaluate their internal controls, identify where fraud could occur, and develop anti-fraud controls and practical data analytics to help surface warning signs earlier.

Whether through a targeted fraud and controls review, ongoing internal audit support, or additional expertise to complement an existing team, having the right perspective can help organizations better understand and address their fraud risks. To learn more or discuss your organization’s internal controls, reach out to your Dean Dorton advisor.