

Improving Automated Controls to Detect Fraud

Over the past 10 years, large and small companies alike have invested money and resources into implementing automated controls—many in an attempt to become more paperless and efficient.

First was the Y2K push, during which companies upgraded, or finally implemented, automated controls. In 2002, Sarbanes-Oxley consultants and auditors drove home the concept that automated controls increase security and reduce opportunity for human error and material weakness.

Automated controls can vary widely from industry to industry, but commonly, they are embedded within software or other information technology tools. In the most simplistic example, a password is a form of automated control.

More complicated controls include process controls embedded within a system. For example, inventory modules can be designed to receive a particular inventory part from a specific vendor. The control might specify that the inventory can only be transferred to a specific location. Take for example, a clothing retailer. The retailer can only buy long sleeve orange shirts from a vendor in NYC. Any purchase order for that particular item with a different vendor will be rejected. When the shirts arrive, they can only be sent to Houston, because market research has shown the shirts will sell particularly well there. By creating these controls, the retailer has removed the purchase order and distribution order checking and double-checking responsibility from the purchaser and automated it.

Automated controls are best used when they take mundane, routine controls out of the hands of employees to allow them to do more meaningful, thought process work. For example, having a purchasing manager review every single purchase order against a vendor price list is time consuming and highly inefficient. Automating the process by creating an electronic form with established vendor prices and a formal electronic review based on purchasing thresholds (which the manager can review and approve) is much more efficient and boosts overall productivity.

However, although automated controls enable efficiency and can handle data at a larger rate than human controls, they do present some risk. The most significant weakness is improper control design. For example, a control might check for a vendor's presence in the system, but may not check whether a vendor is authorized to provide a given product. Outdated controls present

another risk. Employees with high-level access may leave a company, but if their profile still exists, it can be used inappropriately. Controls should be reviewed and tested after any major change in the control feature (such as employee authority), and at a minimum on an annual basis as best practice. Finally, automated controls tend to make employees complacent, and self-checks fall by the wayside. Controls become stale and no longer suited for the purpose for which they were designed. If their output is within expected parameters, they are often not updated or reviewed for ways in which they can be manipulated.

In a worst-case scenario, automated controls present many opportunities for fraud. Corporate fraud most commonly occurs internally, when fraudsters take advantage of complacency in those who oversee the controls. Problems most typically occur when overseers rely solely on automated controls and the historical data they provide, but conduct no further review of the controls or the data they gather, essentially removing the human element from the process.

This case study example highlights the dangers of removing human oversight from automated systems. A company with more than 1,000 employees implemented an employee purchasing system in which each employee was given a Visa card tied directly to the company's bank. The employee would log in to a secure website and code each expense. The employee's manager would then approve the expenses, and the expenses would be posted to the general ledger.

The weakness in this case was that the employees were approving their own expense reports, because manager passwords were not secured. A group of fraudulent employees managed to embezzle thousands of dollars before being caught, and were only caught because the embezzlers were overheard boasting about their theft. In this case, a simple process for tracking unusual changes in spending trends could have prevented this loss. For example, a report that compares current purchases to historical purchases for the past three to six months would have shown the trend. Or, a report that shows all purchases for a specific type of vendor name word inclusions (such as the word spa) or type of item purchased (such as electronics) would also indicate abnormal activity that required further review. Even a simple report showing purchases from restricted vendor types, such as spas or electronics stores, could be used to identify potentially fraudulent activity.

To prevent future incidents, the company implemented a series of human controls that, when coupled with the automated controls, provided the ideal balance of greater efficiency and checks and balances. Each of the steps below ensures that key manual, repeatable controls are incorporated into the control automation process:

- Don't review everything, review for exceptions

Creating a schedule to review for exceptions limits the time typically required to review a large volume of data. In the case study mentioned above, the company established a schedule that reported purchases over 5 percent from the prior 12-month period average for a given employee. From this schedule, the company is able to look further into specific employee expense reports. The employee's typical expenses are also taken into consideration—for example, does the employee typically purchase fuel or airline tickets? Any anomalies are discussed with the supervisor or employee further to eliminate possibilities for fraud.

- Look at trends and investigate significant variances

That same logic can be applied to trend analysis. The company established a base line of regular purchase categories and spending trends by month. When there is a change of a certain category, that expense is investigated. This investigation involves examining data from prior expense reports and justifying the current expense. When unusual trends are identified (such as airline tickets for an employee that typically never travels), the supervisor is questioned regarding the expense.

- Rotate what is reviewed

The company in the case study instituted a rotating review process to alternate a sample of 10 expense reports by department. Reports are reviewed in detail for key items like original receipts. Supporting schedules are compared for validity and missing data. Sample-testing allows for high efficiency and provides a reasonable level of checks and balances on the company's automated controls.

- Eliminate holding accounts

Holding accounts offer few benefits, instead just tempting employees to place amounts in "unknown" categories. The company in the example above had over \$14 million placed in "other expenses" over a two-year time period. The balance in the holding accounts skewed the trend analysis performed on the accounts in which the expenses actually belonged, which could have a serious impact on management's decision making process. Eliminating this category will allow trend analysis by category to be more accurate, and will prevent bad information from being incorporated into the company's financials.

It is also good practice to re-examine the types of accounts being used from time-to-time, to either create new accounts or give guidance on what is appropriate to allocate to each account. Consistency is the key to having good data in the accounts.

The measures detailed above will improve the overall control environment, reducing over-reliance on automated controls by putting the human factor back in the process and lessening opportunities for fraud.

* * * *

Manish Seth, CPA, CFE and MPA, is a Senior Manager with Houston-based Calvetti, Ferguson & Wagner, a full-service CPA firm focused on the energy and multi-national sectors. Its partners represent a variety of industry experience: veterans of Big 4 and mid-tier public accounting firms, as well as CFOs, Controllers and other executive levels. For more information, visit www.cfw-cpa.com.