3-1-2010

Continuous Controls Monitoring Can Help Defer Fraud

Sridhar Ramamoorti
University of Dayton, sramamoorti1@udayton.edu

Joseph Dupree

Follow this and additional works at: https://ecommons.udayton.edu/acc_fac_pub

Part of the Accounting Commons

eCommons Citation
Ramamoorti, Sridhar and Dupree, Joseph, "Continuous Controls Monitoring Can Help Defer Fraud" (2010). Accounting Faculty Publications. 83.
https://ecommons.udayton.edu/acc_fac_pub/83

This Article is brought to you for free and open access by the Department of Accounting at eCommons. It has been accepted for inclusion in Accounting Faculty Publications by an authorized administrator of eCommons. For more information, please contact frice1@udayton.edu, mschlangen1@udayton.edu.
Continuous Controls Monitoring Can Help Defer Fraud

By Sridhar Ramamoorti and Joseph Dupree

The biannual survey of the Association of Certified Fraud Examiners' (ACFE) found that U.S. organizations lose an estimated 7 percent of annual revenues to fraud. Based on corresponding United States GDP figures from the World Bank, this percentage indicates a staggering estimate of losses — around $994 billion — among U.S. organizations, despite increased emphasis on anti-fraud controls and recent legislation to combat fraud.

While there are compelling reasons for monitoring anti-fraud programs and controls manually — there is no question that monitoring activity can benefit from automation.

As the survey suggests, almost every large and small organization is potentially susceptible to fraud risk, both internally from employee theft and corruption, and externally by vendors and other third parties engaged in fraud against the organization.

The recent spate of corporate governance failures further underscores the need to establish strong anti-fraud programs and controls. Organizations have seriously evaluated making fraud risk assessments a mandatory part of internal audit coverage with follow up in areas with a heightened sensitivity to fraud risk.

Many companies have set up separate units to handle potential fraud allegations. For example, Microsoft Corp. launched a Department of Financial Integrity. Most audit committees typically check with individuals from the company's internal audit function as to whether fraud risk assessments have been performed and whether the audit coverage concerning potential fraud risk is adequate, typically as part of their enterprise risk management efforts.

Financial executives realize that fraud remains a largely unmitigated risk because those perpetrating fraud naturally attempt to conceal their tracks, leaving no audit trail. However, manual detection of fraud that is perpetrated within information-intensive transaction processing operations or financial processes is increasingly impractical due to the sheer volume and complexity of the data.

Further, manual detection occurs too late to prevent expensive fraud and its devastating reputational and financial consequences. Controls that use automation are indispensable for detecting fraud within automated operations. As such, and for a variety of reasons, proactive fraud risk management and mitigation efforts must involve automated anti-fraud programs and controls.

However, even if organizations have implemented automated controls, they need to have a way of monitoring these automated internal controls to ensure that they are operating effectively over time. It is in such instances that continuous controls monitoring (CCM) comes in and operates in an online, real-time fashion.

Controls Automation Inadequate, Monitoring is Necessary

The 2009 Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Guidance on Monitoring Internal Control Systems convincingly argues that merely having systems of internal controls in place is inadequate at best, and at worst may provide a false sense of security.

Because unmonitored internal control systems deteriorate over time, it is crucial that they be monitored and their continuing operating effectiveness be validated periodically. Monitoring has the primary purpose of ensuring that internal controls are operating effectively over time.

Just as internal controls can be manually performed, monitoring too, can involve a human agent at every level. For instance, when JPMorgan Chase Chief Executive Officer Jamie Dimon was at Bank One in Chicago, he would ask each employee to evaluate their actions to be taken through the prism of whether they were “unethical, illegal or immoral” and if so, to not take such action or engage in such behavior.

So, while there are compelling reasons for monitoring anti-fraud programs and controls manually — especially because instances like ethical lapses or blatant conflicts of interest are perhaps detected more effectively by human agents — there is no question that monitoring activity can benefit from automation.

Fraud Life Cycle Analytics

In terms of time phase, anti-fraud programs and controls can have a proactive (before the fact) or a reactive (after the fact) orientation. This might be described as the “fraud life cycle,” spanning the phases before fraud occurs, during the
discovery and after the fact fraud investigation and resolution. The period before fraud occurs or gets detected is referred to as the proactive phase; after fraud has come to light, the ensuing investigation is part of the reactive phase.

Continuous controls monitoring of anti-fraud programs and controls can potentially cover both proactive and reactive phases, depending on whether they are preventative or deterrent controls, or whether they are detective in nature. The whole range of data-intensive fact gathering and analysis is referred to as “fraud life cycle analytics.”

More specifically, when contemplating the use of CCM technologies with respect to fraud life cycle analytics, desirable features would include:

- The ability to perform spatial, temporal and statistical data analysis.
- Spatial Data Analysis: For sales agent commission payments, corresponding entries should exist in the geographic or regional financials, including aberrations;
- Temporal Data Analysis: Identify deviations based on historical data and trending over time;
- Statistical Data Analysis: Identify anomalies and exceptions based on characteristics such as missing sequence, outliers, extrapolations, etc.

CCM Capabilities

Monitoring tools generally evaluate one or more of the following, prompting an assessment about the underlying elements of the situation-specific context (adapted from COSO 2009):

- Transaction Data. Highlighting exceptions through comparisons of processed transactions (or master data) against a set of pre-defined control rules;
- Conditions. Comparing baseline or pre-established expectations with actual operations or parameter configurations (system access by authorized users);
- Changes. Identifying and reporting changes to critical resources, data or information allowing verification of authorization and/or propriety;
- Error Management. Monitoring the volume and resolution of activity in suspense areas, error logs or exception reports and the management of the workflow of control exceptions.

To reach maximum effectiveness with respect to data analysis, CCM technologies must possess certain characteristics:

- Compare data and transactions from multiple IT systems and address control gaps that often exist within and between systems. Ability to perform data validation and consistency checks prior to performing a formal analysis avoids the garbage-in, garbage-out (GIGO) problem.
- Work with existing data within operational and financial systems in its existing format regardless of the computing platform, databases and other underlying technologies.

That is, data that is extracted and translated for the benefit of a control subjects the control to greater risk of control error and higher maintenance and ownership costs.

- Nonfinancial operations, key performance indicators, key risk indicators, leading predictive factors and non-numerical data should be within the scope of your controls and CCM technology integration, allowing for a comprehensive approach.
- Apply census sampling for specific target areas — that is, testing 100 percent of the population of transactions in the area of interest. With automated controls and CCM, there is no need to accept the risks associated with sample sets, confidence intervals, selection bias and distribution curves. You can find the proverbial needle in a haystack — and do so proactively.

Genuine monitoring capabilities would demand that CCM is broader in scope; it is IT-enabled online, real-time monitoring that requires an independent, continuous and automated monitoring of controls.

Sridhar Ramamoorti, Ph.D., CPA (samamooti@infogix.com), is a principal at Infogix Advisory Services and serves as technical adviser to FEI’s Committee on Finance & Information Technology. Joseph Dupree (jdupree@infogix.com) leads marketing at Infogix.