



Smart Data Monitoring Can Identify Fraud Indicators and Promote Business Intelligence

A sound governance structure should provide assurance that business transactions comply with management objectives. To be effective, policies and procedures must provide appropriate coverage and an appropriate level of detail instruction to employees who then execute business activities "on their own" on a day-to-day basis. Organizations are thus faced with inherent risk as individual judgment, miscommunication, and other intentional or unintentional deviations can lead to business activity in violation of the policies and procedures. Preventative controls might be designed and implemented flawlessly, however, there always exists such threats as a management override of internal controls - an area the AICPA has called "the Achilles' heel of fraud prevention." Because controls cannot prevent all fraud, after-the-fact monitoring for fraud is a must.

As legislation such as Sarbanes-Oxley and general public sentiment encourage auditors and management to fight fraud, the need for comprehensive fraud detection is greater than ever. Identifying what information, if collected, would help detect fraud is the first step in a data monitoring project. In most cases, this information will be generated by various business transactions that create electronic and paper-based records of the transaction. Historical and ongoing analysis of this record is the essence of monitoring, allowing auditors and managers to begin to detect numerous types of activity that indicate possible variations or problems in the business.

Monitoring of diverse and voluminous data no small task

Technology advances continue to increase the volume of electronic data businesses collect. A study by Keenan Vision estimates online business-to-business transactions occurred 1.1 trillion times in 2004 alone. Each of these transactions likely flowed through to individual companies, generating exponentially more data as ledgers were updated, inventory levels adjusted, accounts reconciled, and descriptive data (e.g. dates, locations, prices) was captured.

By understanding and viewing this electronic record in aggregate, specific analyses can be applied to gain new insights from data. These insights will help identify fraud indicators and promote business intelligence.

The challenges associated with effectively monitoring enterprise-wide data should not be underestimated. For starters, data stores are enormous. According to Experian, companies double the amount of data they collect each year. To minimize the risk of data monitoring project failure, auditors and management should utilize proven methods in their monitoring system; these methods depend on the following: (1) designing a useful data monitoring system, (2) developing a standard and cost-effective rollout process for that system, and (3) capturing business intelligence from collected data. Good execution of the methods above will ensure that monitoring efforts can be appropriately-sized for various business areas, will maximize coverage by automating assessments, and will add value by efficiently providing business information that was not previously available.



In developing a data monitoring program, four criteria should be satisfied; useful data analysis and monitoring systems should be:

1. INDEPENDENT. Information should be analyzed outside of its native system.

Data should be extracted and analyzed with a "sterile" application. Data queried with report writers in their original environment are subject to filters and other database relationships that may have been corrupted, intentionally or not, long ago. In those cases, attempts to tie out financial statement account amounts or to get all of the data in a table may inappropriately indicate that data reconciled, when in fact it should not have.

By extracting data as of a specific date and time, it is also possible to allow others to easily verify results, share the data with other business units, and track changes within specific fields at a later date that may indicate an attempted cover-up by employees. When time is invested in acquiring, importing, and analyzing data, business intelligence analyses should also be run. These might include sourcing and sales analyses or customer relationship management routines that segment and summarize customer data in new ways.

2. POWERFUL. Large volumes of data, spanning entities and time periods, should be analyzed - not just samples.

The keys here are processing power and storage space. Query and data manipulation speed are normally very important because the end-users of such monitoring systems will invariably see results that prompt them to dig deeper or to cross-check data in new areas on the fly. The ability to execute such commands and not have to wait too long for results depends on processing power. The storage aspect is significant because comprehensive monitoring can quickly require manipulation of data with over one million records and one hundred or more fields per record.

3. UNIFYING. Diverse sources of information should be integrated and validated against the business rules.

Once the initial data monitoring project is successful, additional analyses can be added in bolt-on fashion by integrating data from disparate sources such as word documents, email, internet click streams, PC directories, and accounting, operational, and other ERP modules. For example, by comparing disbursement, vendor, and general ledger data, you can identify fraud indicators such as high dollar payments made to newly created vendors with a name similar to an existing vendor that result in charge-offs when entered by the same user ID.



4. **PROGRAMMABLE. Standard, complex, and ad-hoc analysis should be readily available.** Effective monitoring programs should strive to isolate individually dubious transactions and to provide valuable high-level analyses such as trend information on specific ledger accounts, network usage patterns or metrics that can be used to benchmark performance over time. Certain executive users may only need summary information, while other "power" users may wish to advance monitoring efforts with complex statistical tests and artificial intelligence. Standard techniques for fraud detection that can be run on many types of data include regression analysis, minimum-maximum and outlier identification, Benford's Law, joining related data from multiple systems, identifying gaps in sequential data, and graphing to represent relationships between data fields. These techniques make large populations of data easier to understand by subsetting data into small groups of records or fields.

Adherence to the criteria above will support the creation of a data monitoring program that grows with the organization, provides auditors and managers with good information, and leverages the up-front investment in data acquisition and understanding to address business needs beyond fraud detection.

To discuss the fraud and business monitoring aspects of your internal control structure, including the use of innovative data analysis tools and methods, please call Harry Cendrowski, at 248.540.5766.