METROPOLITAN CORPORATE COUNSEL

Seeking a Strong Control Environment: A proactive approach can preempt and detect fraud and misconduct

Books of accounts and records have existed in some form for thousands of years, going back to ancient Egypt and other civilizations in the Middle and Near East, the Zhao Dynasty in the Far East, as well as the Greek and Roman republics in the West. Such record keeping was usually maintained to comply with government taxation requirements. Access to accounts and records was often restricted and record-keeping duties were often segregated as early forms of internal control began to develop. Any record-keeping inconsistencies found through government tax "audits,"1 however, weren't tolerated and carried severe consequences, especially if such inconsistencies were thought to have been committed intentionally.

In today's global economy, multiple regulators, creditors, business partners, suppliers and customers are placing information demands on organizations far beyond those required by the taxing authorities of the past.2 Moreover, donors, and the public in general, are more engaged today than in years past and have similar information requests from not-for-profit organizations and government entities as well.3

These constituencies, as well as boards of directors, trustees, and audit and other committees charged with governance, are all seeking greater transparency and accountability from management regarding the integrity and effectiveness of an organization's internal controls, including how management addresses the potential that fraud will subvert the achievement of its objectives.

The COSO Internal Control –Integrated Framework

The COSO Internal Control –
Integrated Framework4 has become the generally accepted standard for designing and implementing systems of internal control and assessing the effectiveness of internal control.5

While the COSO *Framework* was updated in 2013, its definition of internal control and the components of internal control have remained unchanged from the original framework:

Definition of internal control:

l Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

Components of internal control:

1. Control environment

2. Risk assessment

3. Control activities

4. Information and communication

5. Monitoring activities

Internal control is not unidimensional. A deficiency or a change in one of the components can have repercussions throughout all the components, which should be appropriately addressed by management. For example, risk assessment not only influences the control environment and control activities but also may highlight a need to reconsider the entity's requirements for information and communication or for its monitoring activities.6

Addressing Fraud with a Strong Control Environment

In establishing a control environment, management must consider the potential for fraud in assessing risks to the achievement of an entity's objectives and be knowledgeable about the various ways that fraud can occur. As part of the process for identifying and analyzing fraud risks, management forms a basis for determining how such risks should be managed7 and establishes control and monitoring activities, formalized in policies and procedures, to help ensure that management directives to mitigate fraud risks to the achievement of objectives are communicated and carried out.8

While no control activity can stop a person who is determined to commit a fraud from doing so, a strong control environment, combined with an understanding of the incentives to commit fraud, acts as a form of preventive control against fraud by making the potential perpetrator assess the high risk of getting caught. Conversely, a weak control environment provides opportunity to those thinking of committing a fraudulent act because the risk of getting caught is low.

In this regard, a variety of transaction control activities can be selected and developed to address fraud risk, which in its basic form includes such actions as authorizations and approvals, verifications, reconciliations, and restrictions (physical controls and technology access controls). Segregation of duties and job rotation are typically built into the selection and development of such control activities. Additionally, variance analysis can be used to manage operations and identify possible areas of fraud by directing attention to areas that appear unusual; the preventive control being the establishment of budgeting and standard cost accounting systems that compare actual results to budgets or standards and the detective control being management follow-up in investigating the reasons for a variance from the budget or standard, which may be indicative of fraud, or at the very least require a management response to correct an apparent operational problem.

Pre-emptive Fraud Auditing

The primary factor that distinguishes fraud from error is whether the underlying action is intentional or unintentional. Moreover, attempts are made to conceal fraud. This makes looking for fraud a lot like looking for the proverbial needle in a haystack, or as a recent U.S. Secretary of Defense put it, "We don't know [what] we don't know."9

EisnerAmper's pre-emptive fraud auditing approach addresses the "unknown unknowns" by proactively anticipating scenarios where fraud may occur and designing monitoring activities,10 using data-mining techniques combined with statistical and other quantitative analysis, to identify possible instances of fraud.

Data Mining and Statistical Analysis

Business transactions generate data to accomplish the primary purpose for which it was collected; for example, the preparation of financial statements and various types of management reports. When this primary data is accumulated entity-wide, however, it becomes a stand-alone island of unrelated information, or secondary data.

The objective of data mining is to take disparate data and convert it into relevant information, transforming an organization from an accumulator of unrelated data into a proactive responder to risk.

Data-mining techniques can be developed to look for patterns and trends not evident in large amounts of secondary data, looking for the unknown unknowns in an attempt to draw inferences from such patterns and trends. For example, a database may include data that does not conform to the general rule derived for the data set or the general behavior of other data elements.11

No single professional discipline possesses the knowledge and expertise needed to identify data anomalies that require further investigation. A combination of experts – such as information-technology professionals, corporate and compliance attorneys, subject matter and industry experts, internal and external accountants and auditors, forensic accountants, and financial analysts – and those with quantitative data analysis and correlation skills, such as statisticians, are needed.

Data anomalies are referred to as outliers, and while outliers are usually discounted when making a statistical inference regarding a population taken from a sample, outliers should be examined closely when looking for the unknown unknowns in secondary data. Outliers can be identified by measuring the way data are dispersed around the mean.

Outlier Analysis: Lehman Brothers and Repo 105

On September 15, 2008, Lehman Brothers Holdings Inc. filed for bankruptcy protection. This was an extraordinary turn of events for a company that reported a 2007 fiscal year-end net income of $4.2 billion on revenue of approximately $59 billion and whose stock was trading in the mid-60s less than nine months earlier.

How did this happen? For the complete answer, the reader is referred to the 2,200-page report of Lehman's bankruptcy examiner Anton Valukas, chairman of Jenner & Block.12 This article will focus only on the risk assessment control breakdowns and aggressive accounting applications discussed in the Valukas Report.

Some background first. In 2006, Lehman changed its business model from being primarily a broker and underwriter to acquiring large amounts of investment assets for its own speculation. Moreover, such investments were principally in illiquid assets, primarily commercial real estate, private equity and leverage loans. Lehman's investment strategy continued, and its investment portfolio increased, even during the subprime mortgage crisis that gripped the U.S. economy from 2007 through 2008. This increase in long-term, high-risk investments was at odds with Lehman's own risk management policies.

Lehman was highly leveraged and financed its long-term investment acquisitions primarily with short-term borrowing that needed to be rolled over frequently, e.g., through the use of repurchase agreements. In a typical repurchase agreement, Lehman would enter into an arrangement with an entity that had funds to invest for a short period of time in exchange for

specific securities designated as collateral in an amount in excess of the cash transferred.[13] Concurrently, Lehman would agree to repurchase the securities from the investor at a specified future date at a slightly higher cash amount than the amount received, the difference in the cash amount representing the interest earned by the investor and interest expense to Lehman.

Because of the continued receipt of income from the collateralized securities by the borrower, repurchase agreements are typically not treated as sales of securities but as financing transactions. Thus, the collateralized securities would stay on Lehman's balance sheet, the ownership for which would return to Lehman when it repaid the loan.

What the Valukas bankruptcy team uncovered in its investigation, however, was that for certain repurchase agreements, which Lehman called Repo 10514 transactions, Lehman recorded the short-term collateralized borrowings as sales of its securities. Lehman also entered into Repo 105 transactions at the end of quarterly reporting periods, the effect of which was to show no collateralized debt on its balance sheet, thereby lowering Lehman's leverage ratio. This pleased rating agencies and Lehman's creditors. When the unrecorded debt was paid, the collateralized securities would reappear on Lehman's balance sheet, even though during the repurchase agreement period, Lehman continued to receive interest from its "sold" investments.

The use of outlier analysis could have highlighted an increase in Repo 105 transactions at quarter ends and their subsequent drop-off in activity during the quarters. Using outlier analysis, the dates, the amounts of collateral used and other data regarding the recording of all repurchase agreements would be entered into a program that would calculate the variance around the mean, thus highlighting the days in which the use of repurchase agreements was excessively high, and an examination of the composition of those repurchase agreements would have revealed the use of Repo 105 transactions and how they differed from the standard repurchase agreement.

It is that combination of investigative skills, as previously discussed, and an understanding of management incentives to commit fraud in financial reporting that would have identified what types of transactions were suspect and should be analyzed further.

The outlier analysis discussed above would have at least brought attention to the abnormal usage of Repo 105 transactions at the end of a reporting period and focused attention on an unusual, nonstandard accounting treatment that did not appear to have a credible business purpose and otherwise lacked economic substance.

Points of Focus COSO Principle 8

An organization must consider the potential for fraud when assessing risks to the achievement of objectives

First: Consider the various ways that fraud and misconduct can occur.

1. Fraudulent reporting: When an entity's reports, financial and nonfinancial, do not achieve financial reporting objectives because such reports are willfully prepared with omissions or misstatements.

- **Fraudulent financial reporting:** An intentional act designed to deceive users of external financial reports that may result in a material omission from or misstatement of such financial reports.
- Includes **misappropriation of assets** where the effect may cause a material omission or misstatement in the external financial reports.
- **Fraudulent nonfinancial reporting:** An intentional act designed to deceive users of nonfinancial reporting – including sustainability reporting, health and safety, or employment activity – that may result in reporting with less than the intended level of precision.[15]
- **Illegal acts:** Violations of laws or governmental regulations that could have a direct or indirect material impact on the external financial reports.

2. Loss of assets: Protecting and safeguarding assets against unauthorized and willful acquisition, use or disposal, including

- Theft of assets
- Theft of intellectual property
- Illegal marketing
- Late trading
- Money laundering
- Other related risks:
  - Waste
  - Abuse
  - Neglect

3. Corruption:

- By entity personnel
- By outsourced service providers directly impacting the entity's ability to achieve its objectives

4. Management override: Acts taken by management to override an entity's controls for an illegitimate purpose, including personal gain or an enhanced presentation of an entity's financial condition or compliance status.

Second: Assess incentives and pressures, opportunities, and attitudes and rationalizations. Work incentives may not be aligned with business goals and objectives that, by their nature, create pressures within the organization. Or there are excessive pressures put on employees to achieve unrealistic performance targets, particularly in the short-term, which may be coupled with a weak control environment that creates opportunities for fraudulent behavior, along with attitudes and rationalizations that claim to justify such actions.

David A. Cace, CPA, *Partner at **EisnerAmper LLP**.* david.cace@eisneramper.com

Saurav K. Dutta, Ph.D. *Associate professor in the department of accounting and business law at the **State University of New York at Albany**.* s.dutta@albany.edu

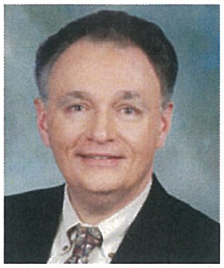
Status and Options

Published

EisnerAmper LLP

http://www.eisneramper.com

Patron
106



David A. Cace

Dr. Saurav K. Dutta

Login to post comments
