

AUDITING

Hidden Dangers In Every Transaction

Lowers & Associates Risk Mitigation White Paper Series



**LOWERS
& ASSOCIATES**
International Risk Mitigation Partners



THE AUDITING FUNCTION: EVALUATING ITS EFFECTIVENESS

BACKGROUND

Larger companies normally have external, independent auditors as well as an internal auditing group. However, mid-size companies might have a very small number (2-3) of internal auditors and rely mainly on an external auditing company to provide oversight of their financial controls. Small companies rarely have any internal auditors and might utilize external auditors only when an “audited financial statement” is required to support an application for a loan. It is the opinion of Lowers & Associates that the internal auditors play a much more significant role in reducing losses than external auditors do. Internal auditors have far greater knowledge of the internal operations of the company. They generally know where the control weaknesses are and which individuals or operations bear closer scrutiny. The auditing function can also serve as a major deterrent to fraud if employees and vendors believe that any significant fraud will be detected quickly by internal auditors.

Lowers & Associates has found that companies that maintain a well-staffed, well-trained, pro-active, management-supported internal auditing function rarely have significant losses. Consequently, it is essential that the underwriter be able to assess the quality of this vital function when reviewing any application for insurance.

TYPICAL/EXPECTED AUDITING OPERATIONAL ELEMENTS

1. The internal auditing function should be as independent as possible.
2. The internal auditing function should report as high as possible in the organizational structure. Ideally, it would report to an audit committee of the board of directors. Reporting to the CEO or CFO inherently creates a conflict if the auditor’s findings reflect negatively on the person for whom they work.
3. The internal auditing staff should have the education, training and experience to be able to adequately audit all functions. For example, auditing of the Information Technology (IT) operations of a company requires a special skill set and internal auditors should have the requisite training or education to properly audit those operations.
4. An annual audit plan should be in place.
 - The plan should be approved by the Board of Directors.
 - The plan should ensure that all financial operations (accounting, purchasing, accounts payable, etc.) are audited each year. In addition, a good plan should



prioritize operational units according to the degree of risk. Higher risk units should be audited on a more frequent basis (at least annually). No organizational unit should go more than three years without being audited.

5. The results of each audit should be reviewed by the Board of Directors and senior management. Senior management should develop action plans for correction of all deficiencies found during audits. The action plan should include timetables for correcting deficiencies and plans for funding if required. Select members of the Board of Directors should form an audit committee to oversee management's response to audits.
 - Are the responses adequate?
 - Is there follow-up to ensure that the reported corrective actions are taken?

Some organizations establish a "Compliance Office" to ensure appropriate action is taken on all audit reports.

6. The internal audit department should be actively involved in the development of internal controls. This is especially important when a company deploys computer programs that integrate the financial operations of a company (accounting, purchasing, accounts payable, inventory, asset management, etc.). The input of internal auditors is vital to ensure that the appropriate checks and balances are in place, that dual control is implemented where required, that "red flag" indicators of fraud are built into the systems, and that adequate exception reporting is included in the software.
7. Auditors should have available adequate exception reports. Exception reports are "red flags" or indicators of possible fraud. An exception report could be issued for each individual action, such as a change to a master vendor list. Or, it could be the cumulative result of a series of actions that produced financial results outside the established acceptable parameter, i.e., the cost of sales reached a level that was outside the pre-established parameter. There should be documentation that exception report items are investigated and the results reported through established channels.

TYPICAL PROBLEM AREAS OR WEAKNESSES

1. The auditing function reports to an executive or operational level that could influence the objectivity of its work.
2. The auditing staff is deficient in size, training, or experience. The most common weakness is size. A review of the audit plan helps to determine whether the size of the staff affects the scope and depth of the audit plan. If the audit plan is weak, the most common reason given is usually the lack of audit personnel.



3. The audit staff does not have exception reports available, or the exception reports are so limited in nature that they serve little use as a fraud detection tool.
4. The audit staff does not have fraud detection software available. Many auditors are not aware of the existence of such a tool. The most common such tool used by the Association of Certified Fraud Examiners is a software package called “ACL for Windows.”
5. Auditors fail to devote sufficient time to auditing two major sources of vendor fraud: consulting services and advertising services.
6. The external auditing company provides consulting services to the client as well as conducting audit reviews.

ESSENTIAL CONTROLS

1. An internal audit department has been established; the department reports to the board of directors.
2. An “audit schedule” has been developed that ensures all essential functions are audited on a regular basis. The audit plan is reviewed and approved by the board of directors.
3. The audit department is staffed adequately and with personnel having the appropriate technical backgrounds.
4. The audit department receives “exception reports” that serve as “early warning” flags for possible fraud.
5. The audit department has available fraud detection software applications and incorporates the use of the programs into the audit plan.
6. The audit department performs year-to-year comparisons of financial statements to detect potential fraud. The following financial ratio analyses are utilized:
 - a. Current ratio
 - b. Collection ratio
 - c. Debit to equity
 - d. Quick ratio
 - e. Inventory turnover
 - f. Profit margin
 - g. Receivable turnover
 - h. Asset turnover
 - i. Average days inventory in stock



7. Audit reports are distributed to the board of directors and senior management; action plans are developed for correction of all deficiencies found during audits.
8. External auditors provide no other services, e.g., management consulting services, to the client.

USE BY AUDITORS OF AUTOMATED TOOLS TO DETECT POSSIBLE FRAUD

The techniques and types of "data mining" techniques in modern audit software are almost unlimited. For example, audit software has can support the auditor's requirement to detect duplicate transactions, missing transactions, and anomalies. Some examples of commonly-used data mining techniques include:

- comparing employee addresses with vendor addresses to identify employees that are also vendors;
- searching for duplicate check numbers to find photocopies of company checks;
- searching for vendors with post office boxes for addresses;
- analyzing the sequence of all transactions to identify missing checks or invoices;
- identifying vendors with more than one vendor code or more than one mailing address;
- finding several vendors with the same mailing address; and
- sorting payments by amount to identify transactions that fall just under financial control on contract limits

Audit software can be used to interrogate a company's data files and identify data patterns associated with fraud. Patterns such as negative entries in inventory received fields, voided transactions followed by "No Sale," or a high percentage of returned items may indicate fraudulent activity. Auditors can use these data patterns to develop a "fraud profile" early in their review of operations. The patterns can function as auditor-specified criteria; and transactions fitting the fraud profile can trigger auditor reviews. Systems can even be built to monitor transactions on an ongoing basis. Continuous monitoring is a proactive approach to the early detection of fraud.

Computerized techniques and interactive software can help auditors focus their efforts on the areas of greatest risk. Auditors can choose to exclude low risk transactions from their review and to focus on those transactions that contain a higher probability of fraud. Audit software also provides auditors with the ability to extract information from several files, with different database management systems, in order to search for underlying patterns or relationships among data. For example, reviewing data from the accounts payable and the contracting databases may reveal a concentration of contracts with one vendor all initiated by the same contracting officer, leading to concerns about possible kickbacks.



Computerized techniques can assist the auditor in identifying symptoms early in the life of a fraud. This will serve to reduce the negative impact of many frauds--before millions of dollars are lost or goodwill is destroyed. Automated routines that monitor key symptoms and track trends can be a major deterrent of fraud, preventing some fraudulent activities and identifying fraud almost as soon as it occurs.

Case Study #1: Contracting Kickbacks

Detection Tools Used: Ratio Analysis

- the ratio of the highest value to the lowest value
- the ratio of the current year to the previous year

How Automated Tool Was Employed: Jonathan, one of the contracting officers, had devised a great win/win kickback scheme. The auditors decided to use digital analysis as part of their review of the contracting section. One of the analyses calculated the total contract amount by supplier for each of the past two years. A ratio of current year to previous year was calculated and the minimum, maximum, average, and highest and lowest five ratios were displayed. While the average was close to 1.0, the highest and lowest five values showed that some companies had significant decreases in business, while others had experienced significant increases in business. The auditors reviewed the details of all companies that had a ratio of less than 0.7 or more than 1.30. Totals were calculated by a contracting officer. For companies with an increase in business, the results revealed that Jonathan had raised many of the contracts. In comparison, Jonathan had raised no contracts with the companies that had seen a decrease in business. The auditors learned of Jonathan's kickback scheme when they interviewed salesmen from the companies that had ratios less than 0.7. Interviews with salesmen from the firms that had increased sales by 1.30 or more added credence to the fraud accusations. Both groups of salesmen said that they were told they would only get business if they paid Jonathan a kickback.¹

Case Study #2: Contract Signing Authority

Detection Tool Used: Benford's Law. Benford's Law, developed by Frank Benford in the 1920s, predicts the occurrence of digits in data. Benford's Law concludes that the first digit in a large population of transactions (10,000 plus) will most often be a 1. Less frequently will the first digit be a 2; even less frequently a 3. Benford calculated the occurrence of each numeral appearing as the first digit and found that it decreased inversely with its value.

¹ Coderre, David. Fraud Detection: Using Data Analysis. Global Audit Publications



How Automated Tool Was Employed: The auditors for Z Company were investigating possible fraud in the contracting section, where thousands of contracts were raised every month. They used Benford's Law to examine the first two digits of the contract amount. The results of their analysis revealed that the digits 49 were in the data more often than expected. Classifying on the contracting officer for all contracts with 49 as the first two digits determined that the contracting manager was raising contracts to \$49,000-\$49,999 to avoid contracting regulations. Contracts under \$50,000 could be sole-sourced; contracts greater than \$50,000 had to be submitted to the bidding process. He was raising contracts just under the financial limit and directing them to a company owned by his wife.²

² ibid



**LOWERS
& ASSOCIATES**
International Risk Mitigation Partners

LOWERS & ASSOCIATES – Fidelity & Crime White Papers

There are three conditions that are present when fraud occurs: Opportunity, Incentive and Rationalization. The information contained in these papers is examples of vulnerabilities and how applying essential controls can significantly reduce the risk of fraud.

About Lowers & Associates

Lowers & Associates (L&A) is an internationally recognized leader in providing Risk Management and Loss Prevention services. L&A provides programs which are designed to evaluate a client's exposure to losses and recommend risk mitigation improvements where such opportunities exist.

Contact Information

Lowers & Associates
125 East Hirst Road
Suite 3C
Purcellville, VA 20132

Telephone: 540-338-7151
Fax: 540-338-3131
Email: info@lowersrisk.com
Web: www.lowersrisk.com