The Evolution of Fraud Investigation
The need for a comprehensive solution

Research Project for Emerging Issues /Advanced Topics Course

Diploma in Investigative and Forensic Accounting Program

Prepared by Rob Shull

June 23, 2003

For Prof. Leonard Brooks

Table of Contents

Objectives

Fraud is not a new phenomenon. Hundreds of years ago, a fraud was perpetrated against eager investors wanting to contribute money towards the expansion of the British Colonies in the South Pacific, in what came to be known as the "South Sea Bubble". While not on the same scale as fraud s of current day, this was a significant event for the day, and certainly not the first occurrence of fraud in the history of man. In recent years the financial community has been severely affected by frauds discovered at companies like Enron, Worldcom, Tyco, Livent, and Bre-X. The economic impact of these frauds has been felt by shareholders and employees as well as entire global capital markets.

The Eighth Global Fraud survey conducted by Ernst & Young tells us that the incidence of fraud has not changed substantially in recent years.[1] Perhaps it has never changed This and other surveys also tell us that our track record for detecting fraud hasn't changed much, either. Why is it that after 1000's of years of commerce, fraud is still occurring, and to some measure, going undetected? Our civilization has advanced to the point where it has become a relatively routine practice to replace a human heart, or to explore far off planets in unmanned space craft, but we still seem to have people rationalizing theft and difficulty catching someone manipulating financial records. Perhaps we need to change our approach. The more we continue to do the same thing the more we are likely to get the same result. Progress requires doing something different. Progress on

---

[1] Ernst & Young, LLP. (January 2003). Fraud: The Unmanaged Risk. 8th Global Survey, 2.

intractable problems not only requires a changed approach, but vision and innovation, as well.

Does this history of recurring financial crime suggest a need for more effective solution? If so, what would the solution look like?

This research paper explores and comments on the effectiveness of current methodologies for fraud investigation. It then takes a broad view of a search for a new, more comprehensive model, drawing on the disciplines of psychology, technology, as well as that of the more traditional investigation.

By compiling this research, I hope to challenge the current state and demonstrate the benefits of a risk-based approach to fraud investigation – specifically incorporating the behavioral aspects of fraud risk, which are sometimes overlooked. I believe that based on the current research, this approach offers a more effective and efficient means of conducting an investigation. This approach has also been lent some weight by the issuance by the Canadian Institute of Chartered Accountants ("CICA") of Handbook section 5135, discussing auditors' responsibility to consider fraud and error in financial statements, and the American Institute of Certified Public Accountants ("AICPA") issuance of Statement of Auditing Standards ("SAS") no. 99, a recent pronouncement on auditors' responsibility to detect fraud.

Introduction

Fraud. The mere mention of the word is enough to capture the undivided attention of executives, board members and auditors around the world. This has never been more so than in the wake of the largest fraud to rock the financial community – Enron. Fraud has

become as much a part of the business environment as computers and stock options. Still, like most parasites, fraudsters could not exist without the proper environment to live and grow. It is this very environment that researchers and investigators rely on to help them understand fraud. By closely examining where fraud lives, why it occurs, how it is perpetrated and how it affects its host, we are better able to understand how to stop it.

Conversely, if we don't understand fraud, it's extremely difficult to identify it. The key to reducing the risk of fraud lies in understanding why it occurs and implementing measures to stop it from happening.[2] If you want to look for fraud, you have to know what it looks like![3]

As we've already seen, fraud is not a new phenomenon. Some people speculate that it has been around as long as industry itself. What's more real is that fraud isn't going away. The results of the Ernst & Young's Eighth Global Fraud survey tell us that the risk of fraud is not new, not obviously changed and still not effectively managed. The complexity of global corporate structures, business transactions and the values at stake for corporations and their executives tend to heighten the risk and consequences of fraud. One of the most disturbing characteristics of fraud around the world is that the majority of the worst frauds are being committed by employees – a staggering 85%. And in over half of the survey responses, the frauds are being committed by management.[4]

---

[2] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 3.

[3] Hodson, N. (1996, Summer). Lead them not into Temptation, *IVEY Business Quarterly*, 1.

[4] Ernst & Young, LLP. (January 2003). Fraud: The Unmanaged Risk. 8th Global Survey, 3.

These results mirror the responses received in Ernst & Young's North American survey of Fraud in the Workplace, conducted in the summer of 2002. In this survey, one in every five Canadian employees said they were personally aware of fraud in their workplaces in the preceding twelve months.[5] This also dispels any faint belief that Canadian employees are intrinsically more honest than their US cousins, who had identical results.

Fraud can impact large and small businesses alike. In a study conducted by the Association of Certified Fraud Examiners on Occupational Fraud and Abuse, the per-employee losses resulting from fraud against small business were approximately 100 times that experienced in larger businesses.[6]

If so many employees have knowledge of fraud at work, why didn't they tell someone about it? Perhaps because nobody asked them.[7] Many of the respondents to these surveys felt that if they were given better means to report such acts, they would have reported what they knew. But in a lot of cases, they didn't. Maybe because they don't think it's their job to report fraud. Maybe because of lingering negative images about rats and snitches. Maybe because it's still not high enough on the corporate agenda. Still, the

---

[5] Ernst & Young, LLP. (August 2002). Press Release: One in Five Canadians Say Fraud Occurs in their Workplace, 1. Retrieved June 16, 2003 from www.ey.com/GLOBAL/content.nsf/Canada/Media_-_2002_-_Workplace_Fraud

[6] Wells, J. (March 2003). Protect Small Business. *Journal of Accountancy*, 27.

[7] Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 30.

message is clear – employee fraud occurs every day, and if you have more than five employees, it is probably happening to you.

While the financial implications of corporate fraud are staggering, the ultimate cost of fraud far exceeds the amounts reported on the evening news.[8] Companies that find themselves the victim of fraud have to face a tremendous loss of investor confidence. This loss stems from the perception that management wasn't doing its job, or that everyone in the organization must be deceitful. The effort that the company must then expend to regain the trust of the investment community can take away from their focus on the corporate strategy, which further affects the financial results of the company. Next comes the negative impact an event like this can have on the morale of the "honest" employees. This can cost the company through drops in productivity, increased sick days, or the loss of valued, experienced staff to competitors. Finally, there are the high costs associated with investigations and recovery.[9]

So, if fraud is a reality, and it has such a significant cost to corporations that are victimized, how can it be stopped?

In the following pages, we'll look at what fraud really is and how it happens. We'll also discuss some of the elements of the current state of fraud detection and how these

---

[8] Ernst & Young LLP. (February 2003). Press Release: It's an Inside Job – Majority of Corporate Fraudsters on the Payroll, 1. Retrieved June 16, 2003 from www.ey.com/GLOBAL/content.nsf/Canada/Media_-_2003_-_Global_Fraud_Survey

[9] Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 1.

elements can be combined with the exciting new opportunities in behavioral research and technology to forge a comprehensive methodology for the future.

Scope of Review

The research conducted for this paper was primarily focused on behavioral studies related to fraud. The concept of behavioral research as it pertains to fraud has been around for some time. It was first widely documented in a theory known as the "Fraud Triangle". The Fraud Triangle is a theory developed by Donald Cressy based on research conducted in the late 1950's. The theory explains how three specific elements interact to permit an individual to commit fraud. This theory explains how fraud is predisposed by the existence of opportunity to commit fraud, the fraudster's motivation to commit it, and his ability to rationalize his actions. Understanding this foundation is crucial to successfully investigating fraud, and the basis for the research in this paper.

Interviews were conducted with experts in Forensic Psychology, Accounting, and Technology Security Risk Services. These interviews brought a unique perspective to the research that extended beyond the materials referenced.

Other references included textbooks and research papers prepared on a variety of topics, including the 'Red Flag' approach to fraud investigations, commentary on the fraud indicators within various accounting streams, and the definition of fraud.

In addition to the references cited throughout this paper, a listing of materials reviewed on the subjects of fraud, behavioral characteristics and investigation techniques is presented at the end of this paper.

A detailed listing of the documents relied upon and the interviews conducted are included in Appendix 1 to this report.

Summary of Findings

The most effective approach to fraud investigation is to use the elements of the fraud triangle to gauge the relative fraud risk in different areas of the organization, then use this information to develop hypotheses, or evidence profiles, about what the evidence would look like if the risk of fraud matured and manifested itself in the records, documents of the company and the experience of its people. The next step is to begin the search for profiles that match the hypotheses.

Through the advances in computer applications, it has become possible to conduct some portion of this search for evidence profiles electronically. This electronic approach cannot only be done more quickly than a manual search, and more cost effectively, but it can be performed on more data that would be feasible if the search was performed manually. The profiles developed in the early stages of the investigation, or even a standard set of profiles, much like the red flags or fraud indicators, can be programmed into data mining tools and volumes of data can be efficiently and effectively searched in a fraction of the time it would take to search them manually.

The fraud risk assessment process gives context to this electronic search. The risks identified in the assessment process form the basis for the profiles of evidence of fraud. These profiles could conceivably be very different from organization to organization, depending on the controls in place, the culture within the organization, etc.

The underlying moral of the exercise is that the act of fraud occurs in organizations with different corporate cultures, by employees with different abilities to rationalize their behavior, and for different reasons. This makes fraud difficult to generalize. Our investigative approaches must be adaptable and dynamic enough to enable us to consider all of these elements if we want to be successful in our efforts. Understanding fraud is the foundation to being able to successfully investigate fraud. In fact, without this basic foundation, the investigation is really little more than an unguided fishing expedition, with little opportunity for calculated success.

By further considering the underlying impact of human behavior, as it relates to the fraud triangle, the overall effectiveness and efficiency of a fraud investigation can be enhanced. The investigation becomes more focused on the areas and employees that could be considered to be more likely to contribute to a fraud risk maturity. This risk based approach also makes the investigation more dynamic, in that the investigation will be customized based on the particular corporate environment, allowing it to adapt to the uniqueness of the industry, system of internal controls and behavioral characteristics of the employees within the organization. This is in contrast to looking for fraud by comparing the facts to fraud indicators - warning signs – that have been developed for known profiles of evidence for frauds that have been previously identified. These fraud indicators limit the ability of investigators to look for new or unconventional frauds as the focus is not on risk, but on looking for evidence found in previous incidents when other frauds were investigated.

What exactly is fraud?

We have reviewed some facts about the history of fraud and discussed the potential for improvements over the current state of fraud detection. Before looking at the specific details of what a new comprehensive methodology might look like, it might be helpful to understand more about what fraud is.

A definition

The Criminal Code of Canada states that a fraudulent act takes place when anyone...

> "380(1) ... who by deceit, falsehood or other fraudulent means ... defrauds the public or any person, whether ascertained or not, of any property, money or valuable security ..."[10]

Fraud is generally thought to be an act of gaining some benefit, or depriving the victim of the benefit, usually financial, by knowingly deceiving someone else – dishonest deprivation.[11] While this is a relatively simple statement, there are two important clues to understanding fraud and how to look for it within these words. First, fraud involves gaining a benefit. This means that there is usually a motive for committing fraud. The motive is usually financial, whether directly or indirectly as in the case of manipulating financial statement information to earn a higher bonus on performance, or a gain on realizing stock options, for example. Still, frauds may range from small-scale cheque

---

[10] Zeir, J. (2001). The Expert Accountant in Civil Litigation, 6, 88.

[11] Greenspan, E. (October 2000). Defending the "F Word", 2.

fraud to multi-national organised crime.[12] Understanding this concept of deprivation and benefit as they relate to fraud allows us to focus our investigation on who may benefit from the act and how this benefit may be conveyed to them.

The second important part of the definition above is the fact that an individual must knowingly deceive someone. This means that fraud cannot be accidental. It's true that an accident may happen that has a similar effect on the person being deceived, but the underlying evidence won't be entirely the same as if the fraud was knowingly committed. This "non-accidental" element of fraud also introduces the concepts of rationalization and opportunity. Rationalization is a term used to describe an individual's ability to accommodate the consequences of their actions without internal personal conflict. For example, a murderer has to believe that what he's doing is really not wrong, despite what the laws may say to the contrary. In a tape recording submitted as evidence during the trial of Paul Bernardo, Bernardo was recorded as saying to his wife, "I'm not really a bad person", indicating that even he needed to believe and to convince others that he wasn't bad. It's a question of subjective morality and the resolution of internal personal conflict. Opportunity, on the other hand, deals predominantly with the factual ability of a person in an environment monitored by electronic and physical controls, to carry out a pre-conceived plan to deceive another person, possibly their employer, without detection. But even opportunity has a subjective element – i.e. the opportunity is as it is perceived in the mind of the individual – this introduces the concept of personal risk tolerance. The fraud triangle is dynamic – for greater reward or need (motivation) people will generally

---

[12] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 3.

take bigger risks by exploiting opportunities that are more tenuous. If moral development is poor and therefore rationalization capability is high, little motivation may be required. Similarly, if there is an overwhelming need, rationalization may easy and extreme opportunities may be attempted.

There have been a lot of studies conducted that look at the minds of criminals and compare them with the minds of "normal" moral individuals. Their objective was to understand the criminal's ability to rationalize their crimes – not how to investigate them. While most people do not equate serial killing with expense report fraud, both actions do require the perpetrator to justify what they are doing. An employee in a company that submits an expense report with a claim based on a fictitious receipt likely understands that what they are doing is against the policies of the company, but yet they do it anyway. They have rationalized their behaviour. It may be that they don't feel they are being paid as much as they should be, so they are trying to make up for this perceived shortfall in compensation by making claims for expenses they haven't incurred. Whatever their reason, the employee in this example has to believe that what they are doing isn't wrong, despite the policies to the contrary.

Restriction of Opportunity is perhaps the best line of physical defence against fraud. By using controls within an accounting system and controls over physical assets, companies can greatly reduce the possibility of a fraud being successfully committed against them. The problem is that tight controls and physical security may also bring the business to a grinding halt. Imagine the impact on productivity if every action by an employee had to be approved by a more senior supervisor, and every supervisor had to report on those actions to a manager, and so on. The time, effort and cost to perform simple tasks would

render the company unable to compete with more efficient competitors and force the company into bankruptcy. There must be a more reasonable approach!

While the elements of motivation and rationalization, being more individually subjective, are not as easily affected by the company for whom the employee works, they can still have an influence on the actions of the employee. Rationalization is a process that can easily be associated with employees that are dissatisfied with some aspect of their job. These employees are then able to commit fraud against their employer because they don't perceive the value system at the company to be consistent with their own. As an example, consider a Canadian taxpayer who fails to declare a small source of income on their tax return. The taxpayer feels that they are over taxed to begin with, and because they are treated so unjustly, by not declaring the income source they are merely compensating themselves for the harsh laws imposed on them by the Canadian Customs and Revenue Agency. There are a range of rationalizations that include: Moral Justification, as above; Trivialization, no one gets hurt, everyone does it, I'm only borrowing; and Transference of responsibility, I was ordered to do it, I would lose my job if I didn't. They may say that if the tax laws were fair to begin with, they would not be forced to cheat on their income tax filing to rectify the injustice. They may say that wealthy people can afford to pay high priced accountants to find loopholes – they can't afford that. They may also have a different view if they thought of cheating on their taxes as stealing from the honest people who do pay their taxes.

Objective of committing fraud

The act of fraud is committed for a purpose. There may be different goals, or motives for the fraudster, but the one that most people think of is money. The objective of fraud forms part of its definition. That is to say that in order for fraud to exist, there must be deprivation.[13] The victim must be deprived of something. This is objective of a fraud. By understanding why people commit fraud, investigators can evaluate the risks of fraud occurring from the perspective of the fraudster.

Often times, the people committing the fraud are only interested in depriving the victim so that they may, in turn gain access to that which the victim is being deprived of. In most cases, this benefit is money. The problem for the fraudster is that no matter how much they try to justify it or conceal it, it's still difficult to turn accounting entries into cash.

The same is true of a fraud where the objective is to manipulate financial statements for some benefit. An example of this type of fraud would be artificially increasing revenues to attain some target, usually resulting in a financial benefit, such as performance-based compensation.

If the objective of the fraud is to inflate operating results, the strategy may be to book fictitious sales of goods. If the sales are fictitious, then it's probably going to be shown as a credit sale. If the fictitious transaction is recorded as an account receivable, even

---

[13] Greenspan, E. (October 2000). Defending the "F Word", 2.

from a legitimate customer, the cash will never be collected. At some point, the receivable will have to be written off.

By understanding the evidence profile from the event that initiates the fraud, in this case, the recording of fictitious sales, through to the entry that conceals what has been done – writing off the account receivable – investigators can focus the search for specific evidence, knowing that at some point, there will have to be some attempt by the fraudster to eliminate the fictitious account receivable.

Fraud and behavioural research

In terms of fraud investigation, behavioural research is a relatively new concept. It has existed in theories about why fraud occurs for some time, but it had never really made its way into the mainstream thought on how fraud should be investigated.[14] Until now. Much of the research conducted on fraud has dealt with frauds that had already been discovered, and the effects of these frauds on the victims. There has been little in the way of approaches to investigating fraud. The common thinking has been that the best way to find a fraud was to examine frauds that have been documented, and look for similar situations.

The Fraud Triangle, a model of the conditions that predispose fraud, developed by Donald Cressy based on research conducted in the late 1950's, is built on the theory of

---

[14] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 78.

fraud as being completely opportunistic and introduced investigators to two new elements to consider during their investigation – motivation and rationalisation. These two elements brought behavioural characteristics of humans into the fraud investigation, and the theory, has gained increasing acceptance in recent years - particularly since the issuance of the CICA's Handbook section 5135 and the AICPA's SAS no. 99.

The 'Fraud Triangle'

The Fraud Triangle is a theory used to explain the conditions that must exist in order for an individual to commit fraud.[15] The three conditions – Motivation, Opportunity and Rationalization – must be perceived to be present by the fraudster in order for a fraud to occur. Conversely, if any one condition of the triangle is absent, the risk of a fraud occurring decreases.[16] This theory has been adopted by the CICA in section 5135 and the AICPA in SAS no. 99. The fraud indicators discussed in SAS no. 99 have been organized to use the three elements of the fraud triangle as a means of identifying areas of high fraud risk.[17] Studies conducted by Zimbelman indicate that the fraud indicator approach presented in SAS no. 82, the AICPA's previous guidance on the auditors' responsibility to detect fraud in a financial statement audit, may not lead to increased

---

[15] Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 30.

[16] Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 2.

[17] Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 31.

fraud detection in all cases.[18] The reason for this is that fraud indicators alone did not alert investigators to the increase in risk, but rather identified instances where a risk might have matured into a fraud, and because of the difficulty involved in presenting a comprehensive list of fraud indicators for which to check, a fraud may go undetected simply because it wasn't included in the checklist.[19] By focusing an investigation on the areas that present the highest risk of fraud, investigators are more likely to identify the evidence of a fraud. This fact was reaffirmed by Wright and Bedard in tests with auditors identifying seeded misstatements in financial statements.[20]

The following paragraphs discuss the three conditions, as seen below, summarised by Ramos (2003) and how they can be used to focus an investigation on the risk of fraud.

---

[18] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 83.

[19] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 92.

[20] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 96.

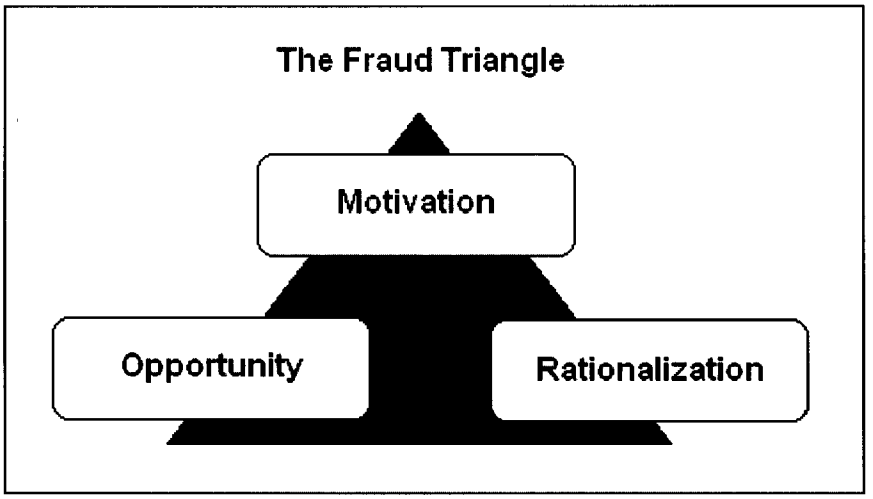

Exhibit 1: Cressy's Fraud Triangle[21]

Opportunity

Opportunity to commit fraud happens when there is a breakdown in the internal controls that allows an employee to do something without detection that they normally should not be able to do. Opportunity can also occur when an employee has identified a means of circumventing the control in place, either through an override process, as in the case of a manager or owner, or subverting the control, for example, by using a stolen authorization code or forged signature. In order for Opportunity to influence the actions of a would-be fraudster, there also has to be a belief on their part that they won't get caught. When they believe they can't be caught, there may not be much need for motivation or rationalization to commit the fraud.[22] Thomas Dalby, a Forensic Psychologist at the

---

[21] Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 31.

[22] Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 3.

University of Calgary stated that a large number of convicted fraudsters have confessed that one of the reasons they ultimately committed the fraud was that it was just too easy.

Internal controls have long been thought of as one of the most effective methods of preventing and detecting fraud. Internal controls convey the message to the entire company that fraud will be detected and that action will be taken against the culprit.[23] In many organisations, management is forced to choose between a tightly controlled environment with redundant controls and a high level of management involvement in day-to-day transaction, and a more streamlined system where employees are empowered to carry out their duties in an uninhibited way. While controls may inhibit the ability for fraud risk, as a result of opportunity, to flourish, the highly controlled environment may also inhibit productivity, innovation or employee morale. Similarly, an environment with absolutely no internal controls may demonstrate trust and promote entrepreneurialism, but the lack of controls leaves the assets of the company vulnerable fraud. Management must find a way to balance these two competing imperatives. If this balance is not achieved, the opportunity for a fraud occurring increases or the organization becomes less efficient and less competitive. "Prevention is better than a cure. However ... there is more often than not an internal control which should have prevented or detected the

---

[23] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 15.

crime, but it was either overridden, or not properly understood by the staff responsible for the control."[24] Of course, opportunity is more than circumventing controls.

Opportunity can also exist with authority. Senior individuals in organisations often have greater control or authority to effect transactions, or to gain access to assets. In most cases, this is necessary to permit the effective operation of the company, but it can represent a threat to the company, as well.

How does this impact an investigation?

In order to understand how opportunity fits into an investigation of a suspected fraud, the investor must ask a simple question: "How would I carry out a fraud and not be detected."[25]

A good place to start is with an assessment of the internal controls. When investigating a known fraud, it's easy to focus on the controls that should have stopped the fraud from taking place. By working back through the system of internal controls and identifying how they were subverted, the investigator gains valuable clues as to whom the perpetrator may be. With most controls, there are few employees that have the ability to simply override them. These employees are typically management level, at least. Employees who have a thorough understanding of a particular control are often the most

---

[24] Ernst & Young LLP. (February 2003). Press Release: It's an Inside Job – Majority of Corporate Fraudsters on the Payroll, 1. Retrieved June 16, 2003 from www.ey.com/GLOBAL/content.nsf/Canada/Media_-_2003_-_Global_Fraud_Survey

[25] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 14.

knowledgeable about how the control could be subverted. Depending on how the fraudster is suspected of breaching the control, there may be a relatively small group of people who have the "opportunity" to actually commit the fraud.

In smaller businesses, internal controls are not generally as effective. This is largely due to the smaller number of employees among which to segregate duties. Another reason is that in smaller businesses, employees tend to know one another and there is a higher degree of trust.[26]

If the investigator is looking for possible risk of fraud, the approach is similar. By working back from the goal, you can gain an understanding of what would have to be done to successfully attain that goal, and who has the authority or ability to cause that action. This is the profile of the evidence.

Consider a simple case of embezzling funds. The goal of the fraudster is generally to get cash out of the company. It may be that the only way to do this is to negotiate a company cheque. The goal then becomes getting a cheque generated to a payee of some sort, and getting the cheque signed. The controls over this process may mean that there are extensive embedded controls in the payment stream software used to generate cheques. The fraudster then has to contemplate altering a legitimately generated cheque for his or her own benefit, setting up one or more fictitious suppliers, or perhaps causing a manual cheque to be written (an easy way to circumvent electronic controls). Any of these three alternatives could then become the fraudster's interim goal. If the choice is to alter a legitimate cheque, the fraudster then has to intercept the cheques after they are signed,

---

[26] Wells, J. (March 2003). Protect Small Business. *Journal of Accountancy*, 27.

but before they are mailed to the legitimate suppliers. It may be that anyone in the company could have taken the money, but only a handful of employees had the access and opportunity to handle the mail prior to having it picked up in the mailroom. This example is meant to demonstrate that by tracing back though the steps necessary to commit a fraud, the investigator is able to make an assessment of the opportunity to do so. Combining these assessments from many different hypotheses of how a fraud may be perpetrated can paint a picture of how the element of Opportunity may contribute to the risk of one or more of these hypotheses of fraud maturing into an actual fraud.

Finally, special attention should be paid to instances where an employee, usually a senior employee, creates an opportunity by asserting authority. This may be where a supervisor overrides a control, or a less obvious situation where a senior person takes on responsibility for a more clerical function, such as a bank reconciliation, in order to subvert the segregation of duties that are the key to so many internal controls. In a case like this, there may be an informal understanding between the supervisor and the clerical worker – one that will not be documented in any assessment of the internal controls. The supervisor will usually provide the clerical worker with a plausible excuse of confidentiality or some other circumstance that requires direct management involvement. Once this understanding is in place, the supervisor may now have the opportunity to authorize a payment, for example, and then manipulate the bank reconciliation to conceal the disbursement.

Motivation

A desperate need is often enough to cause a trusted long-term employee to turn on their employer and take the risk of committing a fraud.[27] This intense need could be related to a family emergency, or a dependency, such as drugs or gambling, which demonstrates the subjective nature of opportunity. In these cases, the employee may be willing to accept the risk of getting caught and going to jail because they feel the value of getting access to the benefit involved far outweighs the risks. Motivation alone may be enough to heighten the risk of a fraud occurring.

Perhaps the image of motivation that most often comes to mind is the pure financial gain. An employee that successfully defrauds a company of any significant amount could be said to have been motivated by greed, or at the very least, the want of material possessions.[28]

In some circumstances, the sheer excitement of committing the crime, or the feeling of superiority the fraudster feels for having duped the controls system is a form of motivation. Motivation based purely on some non-financial basis is not typical among conventional fraudsters, but this type of motivation can be extremely powerful, according to Dr. Dalby. Here, again, the close relationship between the conditions in the fraud triangle becomes important. There is undoubtedly a dynamic interaction between rationalization and motivation – excitement and revenge may provide bases for

---

[27] Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 2.

[28] Zeir, J. (2001). The Expert Accountant in Civil Litigation, 6, 91.

rationalization as well. The thrill and the satisfaction that must exist for motivation and rationalisation can be achieved without profiting personally. Two examples of this type of non-financial "profit" are the computer hackers that penetrate computer networks and the people that infect these networks with computer viruses. While these acts can more closely be related to acts of vandalism, rather than fraud, the possibility does exist for individuals to commit fraud to gratify their egos, rather than pad their wallets.

There is another form of motivation that is not quite as direct as this. Consider the motivation of an executive to show revenue growth in a period of economic recession. Many organizations today have aggressive growth objectives and the managers that execute the strategies to achieve the objectives are well rewarded for success, but failure is unforgivable. This type of motivation stems from a corporate environment.[29] Pressure.

Motivation is something that influences our decisions to act in a certain way. It can be something that is completely different from person to person, or it can be something that is woven into the fabric of the corporation. In the example above, the pressure to meet certain financial targets may motivate efficiency and effectiveness. For some there may be enough motivation to engage in questionable financial reporting.[30] For others, it may be a sign that they don't fit with the corporate culture.

---

[29] Young, M. (2002). Accounting Irregularities and Financial Fraud, Second Edition, 1, 3.

[30] Young, M. (2002). Accounting Irregularities and Financial Fraud, Second Edition, 1, 12.

Motivation is often associated with incentive.[31] It's common for executives to be rewarded for driving a company to achieve the target, or sanctioned for failing to meet that target. Either way, this type of motivation can influence actions, and heighten the risk of manipulation of financial results in order to get the company the last few steps to the goal.

How does this impact an investigation?

An investigator should be alert for both positive and negative incentives in an organisation. Any employee whose compensation is closely tied to some measure of performance may be motivated to make decisions that positively impact the measure. Therefore, one objective of an investigator should be to identify the motivations that exist in a company. These may include stock options, performance-based compensation, aggressive revenue or growth targets, or simply a demanding environment that requires above average performance just to keep a job. These situations are all related to the work environment.

Many motivations exist on a personal level. These motivating factors are more difficult to identify because they could be different for every employee in the organisation. The most acceptable way to probe the motivations of individual employees is through conducting interviews. These interviews require a certain approach that allows the interviewer to gain the trust of the interviewee to the point where talking about such

---

[31] Landsittle, D. (2002). Detecting Financial Statement Fraud: Proposed SAS 82 Revision. 2002 Symposium on Auditing Problems, University of Kansas, 48.

motivations doesn't cause the interviewee to get their guard up. If this type of interview is successfully conducted, it can lead to valuable insight into a person's motivational influences. Often times, intense motivations, such as urgent need for money, perhaps as a result of some unforeseen adversity, are the first to surface. It may be that the subjects of the interviews are subconsciously beginning to seek empathy from the investigator, or because they continuously need to remind themselves of why they committed the fraud in order to reaffirm their rationalisation.

The investigator must listen carefully for signs of desperation or need in both the words and the tone of the voice as the interviewee responds to questions. Other clues could include expensive tastes that are not typical for employees at a certain level. These expensive tastes may provide the motivation to commit fraud. More personal circumstances, such as drug or gambling addictions are difficult to glean from an interview. The subject will likely be guarded as their addiction may be a source of embarrassment or simply something they realise is better kept out of the office. If the addiction is prevalent enough, there are likely other employees that have their own suspicions, and it may have come to the attention of management.

After collecting information about the various motivations that face potential fraudsters, the investigator must weigh them to see if any of them present a heightened risk of fraud. It may well be that individually, the motivations seem trivial – after all, who wouldn't like to dress well or own an expensive wristwatch. The real risk comes when these motivating factors combine with factors from the other fraud triangle conditions.

Rationalization

Rationalization is one element of fraud risk that can stem back to the earliest years of a potential fraudster's life. Life experiences dating back to how parents and friends behave affect a fraudster's ability to rationalize – at least in a moral sense. These influences carry through to the culture at the organisation at risk. If senior management has a tendency to disregard the rules "for the good of the company", the employees will learn that in some cases rules really are made to be broken. If they are uncomfortable with this practice, there is a misalignment of values. The employee will feel that they are nothing like the people they work for and so stealing from them will be easy to rationalize. Value alignment is in some ways like belonging to the same family. In the example of the taxpayer discussed earlier, the taxpayer would likely find it easier to cheat on their tax return, than to steal from their child's piggy bank, because they share the same values as their child – the are working toward a mutual goal of benefiting the family. So, if the employee feels that senior management is not concerned with his well being, then the employee will not feel as though they are part of the "family", and will likely act in a way that benefits himself first, and the corporation last, if at all. Similarly, if the employee agrees with management's philosophy, they are more likely to bend the rules for their own personal benefit.

Rationalisation occurs when a person is able to resolve the moral conflict they feel about committing a fraud to the point when they feel they have done nothing wrong, and that they are still an honest person. No one wants to believe they are dishonest or untrustworthy. This rationalisation can come through a variety of means. Many employees convince themselves that the need for the money is temporary and that they

will pay it back. No harm done. Others believe that they need the money more than the company does. This takes us back to motivation. In the case of a disgruntled employee, the feeling is often that they simply deserve it. Perhaps they didn't get a raise in pay or the promotion they were expecting. Maybe they feel they work harder than everyone else and aren't paid enough. Whatever the reason, Dr. Dalby states that a person typically has to come to grips with the moral issue of stealing before the risk of them committing a fraud will increase.

Rationalisation is such a powerful element in the fraud triangle, that if a fraudster has a strong ability to rationalize his actions, they may not need much motivation and they will actively search out and exploit an opportunity.[32]

One aspect of rationalisation is being able to accommodate the risk of getting caught – or if you get caught, of suffering any serious repercussions. Studies show that corporations often choose not to prosecute fraud to avoid embarrassment. The fear of adverse publicity, the perception of customers and shareholders, or perhaps just the embarrassment of having to admit that you fell for one of the oldest scams in the book are enough for most victims of fraud to quietly dismiss the fraudster and hope it never happens again.[33] As a consequence, fraudsters go unchallenged and are able to repeat their scams and hone their skills. Indeed, many organisations consider some level of fraud as the "cost of doing business."[34] This is evident in retail sales. Many stores

---

[32] Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 3.

[33] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 4.

[34] Ernst & Young, LLP. (January 2003). Fraud: The Unmanaged Risk. 8th Global Survey, 2.

include an expense on their financial statements that they euphemistically refer to as "Inventory Shrink." What this really shows is the cost to the store of thefts from shoplifting and other supply chain theft. The institutionalization of fraud in this way tells employees that the company expects that losses to some degree will happen – that they have accepted it as a cost of doing business. Since the company is expecting it, the employees can more easily rationalize helping it along.

How does this impact an investigation?

It's difficult to know with any certainty what a person's moral or ethical values are. Rather than attempting to evaluate the morality of every employee within the organisation, it's more relevant, in the context of a fraud investigation, to remain aware for situations or circumstances that may present a heightened fraud risk.[35] In SAS no. 99, the AICPA requires auditors to make inquiries of management. It also encourages auditors to expand the scope of their inquiry to other individuals in the organization to corroborate responses.[36] In conducting a fraud investigation, interviewing people in the organization is one of the principal evidence gathering procedures. This is the context in which a broad evaluation of this element of the fraud triangle can occur.

Misaligned values are a clue to a fraud suspect. This misalignment doesn't just occur in new employees. Studies show that employees or management of a company – frequently trusted employees who have been with the company for many years – perpetrate the great

---

[35] Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 31.

[36] Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 30.

majority of the worst frauds.[37] This misalignment may be at a personal level, where the employee feels that the company owes them more for doing their job. To this end, an effective investigator might look at promotion announcements and find out who it was that just didn't quite have what it took. In the mind of a fraudster, being passed over for a promotion is a common way to rationalize taking back what should have been theirs in to begin with. This type of rejection also seems to define the employee as not really being good enough for the company – isolating them, setting them apart.

Rationalization may also be a more widespread corporate problem. It's been said that corporate culture and corporate values, such as "client service", "quality", or "value" are set at the top. So too are negative values, such as "it's ok to cheat a little", or "do what needs to be done, no matter who gets hurt." A corporate culture, or even the perception of a corporate culture like this makes it easy for employees to rationalize their actions in fraud. It becomes a mentality of "everybody's doing it", or "my boss does it." In cases like this, employees who commit fraud are doing exactly what they have been taught to do by their supervisors. They feel that if they don't do it, someone else will, anyway. This mentality can often be very costly if combined with ineffective internal controls that provide the employees with abundant opportunity to commit fraud.

Generally, a corporate culture that condones these actions is pretty easy to spot. It will come across clearly in discussion with management and supervisors who may even be proud or boastful of the controls they have overridden to "get the job done."

---

[37] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 5.

How the elements of the Fraud Triangle work together

Once the investigator fully understands the three elements of the fraud triangle, the next step is to understand how they work together to help identify heightened fraud risk. The object is to look at the opportunities that exist and the motivations and rationalization of the people working there.[38]

We said earlier that the three conditions of the Fraud Triangle must be present in order for fraud to occur, demonstrating a heightened fraud risk. The fraud triangle, however, is not a static model. This is a somewhat misleading aspect of the preceding graphic representation of the model as a triangle standing on its base, which conveys a sense of stability. Steve Albrecht's representation of the model contemplates the three predisposing elements as movable weights on a three-tiered balance. It is an effective but inherently unstable and dynamic model. If anyone of the conditions is not present, fraud does not occur even though the other two may be present. A strong motivation and an opportunity may be balanced by a strong moral development that will not permit rationalization to occur. If an employee is promoted to a supervisor position, and is now trusted with the physical access to the cash drawer, there is an increase in opportunity – they can now reach out and touch the cash, where before they could only see the locked cabinet in which it was kept. In their prior position, the lack of opportunity balanced out the employee's motivation and ability to rationalize. Now, with the increase in opportunity, the same ability to rationalize and the same motivation could turn this situation into a higher risk for fraud.

---

[38] Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 3.

Now consider what would happen if the same employee found out that their child had gotten into trouble with a gambling addiction and owed some not-so-reputable people a lot of money for gambling losses. This would represent an increase in motivation – this employee now needs the money to save his child from potential harm. With two elements of the fraud triangle now out of balance, the risk of fraud in this situation has again increased.

Now consider the employee's ability to rationalize. The employee feels that if they took the money, they could pay it back before anyone found out. No one would know or be hurt. It would a temporary loan. What's more, the promotion they just received came with a small pay increase that could fund the repayment over time. Let's now assume that our supervisor finds out that the job he is doing was formerly split between two people who had been let go as part of a headcount reduction plan. He now feels that the company has taken advantage of him and owes him this temporary loan. This situation has just turned into a high risk for a fraud occurring. The progression is not unrealistic, and the example shows how the risk of fraud can increase if the conditions of the Fraud Triangle do not maintain sufficiently positive status – that is low opportunity, low motivation and low rationalization ability.

In our first example, if there were an offsetting change in one of the other elements of the triangle (motivation or rationalization) the increase in the opportunity may not present a heightened risk at all. Consider how the situation may have been different if our supervisor received his promotion, and significant additional compensation in the form of performance based bonus and a raise. This may offset the increase in opportunity. He may not be able to justify the risk of losing his higher paying job. He would essentially

be stealing from himself. This alternative outcome demonstrates the importance of monitoring the elements of the fraud triangle and ensuring they are kept in some form of balance.

Other Clues

Look for the unusual

To condense the concepts discussed above, the basic approach to identifying areas of significant fraud risk, the investigator should be alert to any of the elements that appear out of the ordinary. While it may not be unusual for different people within an organisation to have different degrees of responsibility or opportunity, these factors should be balanced by factors that mitigate the risk of fraud. Cases where employees are doing far more than anyone else at their level in the organisation could demonstrate a higher degree of opportunity as they begin to bridge roles that once relied on segregation of duties for control.

Repeat Offenders

Fraudsters are generally not content to commit fraud just once.[39] This could be because once the three conditions of the fraud triangle are all present and the risk of fraud increases, it is unlikely that any action will be taken to correct the situation unless the problem becomes known to the organisation. This leaves the door open to the fraudster

---

[39] Davia, H., Coggins, P, Wideman, J., Kastantin, J. (2002). Accountant's Guide to Fraud Detection and Control, Second Edition, 2, 45.

to continue perpetrating the fraud over and over again. Dr. Dalby stated that when he had interviewed former employees who had been prosecuted for fraud against their employer, he asked why it was they didn't stop the scheme when they realised what they were doing was wrong. Some of the people said they enjoyed the excitement it brought into their boring jobs, and others just wanted the extra income. The answer he received most often, however, was that they realised they were likely going to be punished in some way if they were caught no matter if they stopped now or not, so they continued with the scheme to see how long they could keep it going.

A further element to the interaction of the predisposing conditions for fraud is how rationalization and motivation work together to address the question that frequently arises in investigations – "If he was doing this what else was he doing?" Practical experience suggests that frequently a perpetrator has exploited more than one opportunity. If they have demonstrated the motivation and the ability to rationalize an act of fraud, what stands between the company and other fraud? Experience suggests, other opportunities.

Behaviour in an Interview

In many cases employees that are being interviewed as part of a fraud investigation are nervous, even if they have nothing to hide. Dr. Beaulieu has conducted research into the behavior of individuals in an interview environment and found that it may be more difficult than many investigators think it is to tell when someone is lying. That is one reason why it is important to observe the interviewee closely. Comments are sometimes made that provide insight into more than the question being asked. Listen to the tone of their voice. Are they being dismissive? Are they agitated? Are they anxious? Are they

being defensive? All of these factors may have different meanings in different situations, but they may provide some insight into the interviewee's perception of what they may have done wrong, which may provide insight into their ability to rationalize a fraud, if they have committed one. For example, an employee who admits to insignificant infractions, such as making long distance calls on company phones, or using company postage for their own use, either by stating their involvement, or by implying that these things are not important and that everyone does them, may have already decided that these are just a few of the things that the company "owes" them. If this is the case, they may be willing to rationalize much more significant actions, such as expense report fraud, or theft of more significant assets.

E mail

In a study released by the META Group in April 2003, a survey designed to identify the preferred method of business communication showed that business people surveyed believe e-mail to be more valuable than the phone for business communication. Among the reasons cited is the fact that e-mail provides an instant record of the transaction. In fact, approximately 80% of respondents felt that e-mail was the one communication tool they would least like to be without.[40] This provides a significant opportunity for investigators of all sorts, including fraud investigators. As most business systems are now electronic to some degree, a great deal of information processing is done at a

---

[40] META Group. (April 2003). Press Release: 80% of Users Prefer e-mail as Business Communication Tool, Says META Group, 1. Retrieved June 16, 2003 from domino.metagroup.com/pressHome.nsf/(webPressRelease)/D279165CF57E398785256D10004C9B41

computer terminal. Often approval for these transactions is done using the electronic user identification and password to verify the authority of users and approvers. In the case of overrides of these controls, however, e-mail is a favorite alternative method for giving the authorization to proceed with a transaction. This may be because when someone is doing something that is inherently dishonest, they don't want to have to look people in the face and tell them to break the rules, or it may be that people simply don't know the extensive data trail a simple e mail message leaves behind. With 80% of all business people using e-mail for day-to-day interaction, the automatic records that are being generated offer a valuable look at what may have happened leading up to a fraud. Also, this electronic evidence can often be tied back to a specific user, through network security protocols and passwords.

Written evidence is valuable for other reasons. Because, according to Dr. Dalby, the human mind is predisposed to not *want* to lie when we write about events or reasons for unusual entries, as in e-mail, we tend to include too much detail in our discussion. This stems from a desire to convince the reader of what we are writing about – to rationalize behavior with a perception of the facts. In the normal course, backed by the legitimacy of the request, we would tend to write in order to simply convey a message. This subtle difference is now captured forever on the electronic back up tapes of corporate e-mail servers everywhere, waiting to be discovered.

Investigative Techniques

Johnson et al. (1993) conducted several studies on the impact of behavioural research in fraud detection and found that the highest success rate in audits occurred among auditors

using a combination of cues to develop a mental representation of the fraud. By understanding the behavioural aspects of the Fraud Triangle, these investigators were more successful in discovering fraud.[41]

While the two different approaches discussed below are both commonly practiced by investigators, there are inherent weaknesses in each approach in isolation. In some instances, these approaches are even confused for the same approach. This is not the case.

Risk Factors

Risk factors are often the first link in the evidence chain even before red flags. Risk factors are not mean to be indications that there is a problem, as is the case with a red flag, but rather that there could be a problem. The difference is similar to being at risk of having a heart attack – overweight, smoking heavily, drinking excessively – and experiencing chest pain. In the first instance, you may never actually have a heart attack, but the circumstances you put yourself in are consistent with the conditions that predispose most heart attacks. As an example, a risk factor relating to fraud might be that a company has no controls in place over processing invoices to suppliers. An indication of fraud occurring would be that invoices from one supplier that is unknown to the buyers

---

[41] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 84.

in the company have been processed with no indication that the related goods were ever ordered or received.

A "Red Flag", on the other hand, is a signal that the evidence is consistent with what would be expected if a fraud risk matured. It's a warning sign that a fraud may have taken place, or is in progress. While the term is used indiscriminately in literature to describe an indicator of risk as well as an indicator of risk maturity, for purposes of this paper, the term is defined as the latter – an indication that a risk has matured.

Once a risk factor is identified, the investigator must evaluate the strength of the relationship between a given risk factor and the likelihood of a fraud occurring. In some instances, the risk factor identified might not be that significant, or the risk of fraud might be mitigated by some other factor not yet considered. These risk factors serve to point the investigation in the right direction – to focus the attention on the areas where a fraud would most likely be taking place.

Risk factors can relate to motivation, opportunity or rationalisation. In combination, risk factors covering more than one element of the Fraud Triangle can demonstrate a much higher risk of fraud than the presence of a single factor.[42] This relationship underscores the theory that just because the opportunity to commit fraud is present, there still may not be a high probability of fraud occurring. After all, evidence suggests that the overwhelming majority of people are predominantly honest and trustworthy. In the Ernst

---

[42] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 85.

& Young workplace fraud survey over 80% of respondents said they would report a fraud if they had an appropriate means to do so.[43] However, if all three conditions of the Fraud Triangle are elevated – opportunity, motivation and rationalisation – there is a higher probability that fraud may be occurring.

The next step of an investigation is to consider these risk factors and to begin to identify the indicators of mature fraud risk, which have come to be known as 'red flags'. As discussed earlier, this step takes the areas of risk and draws hypotheses about what a fraud may look like if the risk were to mature. It creates its own profile of the evidence the investigator would expect to find if the fraud was actually happening. It is useful to relate this step to an analysis of the potential exposure the company faces to fraud risk, considering the specific conditions of motivation, opportunity and rationalisation that exist within. A sample of such a summary is included at Appendix 2 to this paper.

An approach that focuses on risk factors is more flexible and adaptive to the dynamic nature of fraud. There have been countless different variants of schemes used by fraudsters to gain benefits from their victims over the years. By focussing on the circumstances that would permit fraud to occur provides a more complete look at the environment and is more likely to lead to discovery of the fraud, if it exists. Wright and Bedard (2000) show that auditors that considered the risk factors indicating a heightened

---

[43] Ernst & Young, LLP. (January 2003). Fraud: The Unmanaged Risk. 8th Global Survey, 2.

risk associated with incentive, or motivation, and opportunity to commit fraud conduct investigations and tests that are more effective at uncovering fraud.[44]

'Red Flags'

A red flag approach to investigation essentially looks at the evidence of known schemes and compares them to the evidence available to the investigator in the case at hand. If the conditions and evidence of the known fraud is in fact similar to the currently suspected fraud, there is likely a fraud taking place. In the example above of the symptoms of a heart attack, a patient experiencing chest pain and shortness of breath is likely not at risk of having a heart attack, but rather *having* a heart attack.

Many people confuse these two concepts, namely risk factors and red flags, or warning signs. The terms are often incorrectly used interchangeably. Investigators have to be clear on the differences between risk factors and warning signs as, individually, they have limitations in their evidentiary power, and in how they should impact an investigation, but if used in conjunction with each other, they can result in an effective and efficient approach to identifying and investigating fraud.

Risk factors offer investigators a clue as to where in a company a fraud may be most likely to be perpetrated, whereas red flags offer specific evidence profiles of known frauds for the investigator to compare to the evidence on an existing investigation. While

---

[44] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 95.

red flags – the chest pains of the investigation – offer a good indication there is a fraud occurring, risk factors offer only an indication that there may be a problem. Just because you are a smoker doesn't mean you will absolutely have a heart attack.

This approach adds structure to the investigation process and is designed to make data collection and summarization more comprehensive and uniform. Users of this approach, however may tend to overlook important facts not addressed by the checklist, namely behavioural aspects.[45] For example, if a fraud was taking place at a company under investigation, but the exact *modus operendi* had not been previously documented and included in the list of possible warning signs, evidence of the fraud may be overlooked by the investigator.

Perhaps another view of the red flag approach in relation to the elements of the fraud risk approach is that the red flag approach can be used as another means of identifying fraud risk. The studies conducted indicate that the red flag approach is simply not as comprehensive as the fraud risk approach. If, however, the red flag approach is used to identify instances of fraud that do match the profiles of expected matured fraud risk, this result is itself an indication of heightened fraud risk. If you have discovered evidence suggesting that a fraud is being perpetrated by an employee, is that not a strong signal that there is a higher risk of fraud in the areas of the company over which that employee has access? Is there any stronger signal? In fact, the results of the red flag approach tell

---

[45] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 92.

the investigator that more attention should be devoted to investigating the elements of the Fraud Triangle as they relate to this employee, as he has already demonstrated the ability to rationalize his actions, and that he seemingly has a motivation to commit fraud, so the probability is high that if he is given the opportunity to commit other frauds, he will take it. When an investigator first identifies a fraud, the next question frequently is, "If the employee is doing this, then what else is he doing that I don't know about?"

This argument further goes to demonstrate the merit of integration between the two approaches. It is obvious that to apply the red flag approach without considering the fraud risk approach would be detrimental to the investigation. Combining the approaches and giving consideration to the behavioural aspects of the employees in the organisation when conducting the investigation would enhance the result of the investigation.

Common examples

The following paragraphs look at some common examples of red flag indicators of fraud in an accounts payable system. Additional red flag indicators can be found in Appendix 3 to this document.

Address Warning Signs

When an employee creates a fictitious supplier with a view towards having disbursements made to the supplier for goods that don't exist, there are some common profiles that emerge.[46]

---

[46] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 9.

Post office boxes are a common tool used by fraudsters to perpetrate their schemes. This is a relatively inexpensive means of giving the appearance of legitimacy to a fictitious supplier. The very presence of vendors with a post office box used for correspondence and receiving payment is a warning sign.[47]

For a similar reason, vendors with notes in the master file that indicate payments for invoices will be picked up in person, should also draw special attention. This is another clue that the vendor may not exist for any reason other than to collect cheques![48]

Some less sophisticated schemes have the fictitious supplier appearing to share office space with the employee that set the vendor up in the first place. By comparing addresses in the vendor master file with those of the employees of the organisation, such a scheme can be easily identified as a warning sign of fraud.[49]

Similarly, truly ambitions fraudsters may create several fictitious suppliers to double, triple or even quadruple the value of invoices that the victim may pay. Vendors that appear in the master file to share addresses with each other, or with employees are another warning sign.[50]

---

[47] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 10.

[48] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 10.

[49] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 10.

[50] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 11.

Document Warning Signs

One of the biggest clues to a potential fictitious supplier fraud is the invoices issued for payment. There are several things to watch for with respect to invoices. Any one profile or a combination of profiles may be present.[51]

Many times the invoices themselves received from the fictitious supplier will be authentically produced invoices, often from a local print shop. These invoices are usually sold in lots by the hundred or thousand. They also tend to be consecutively numbered. If invoices received from a supplier are sequentially numbered, it may be an indication that the supplier has only customer, or it may be that the supplier may be fictitious.[52]

Shuffling the invoices can sometimes conceal this warning sign. The perpetrator will mix the invoices up so that there is not a sequential series of invoices sent to the victim. This attempt at masking the fraud actually results in another warning sign – invoices that are not in chronological order.[53]

Invoices whose numerical sequence does not match the chronology of the period in which they were issued indicates that the supplier either does not have very strict policies with respect to issuing invoices, or that there is an employee perpetrating a fictitious supplier scheme that is not willing to waste unused invoices![54]

---

[51] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 13.

[52] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 13.

[53] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 13.

[54] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 13.

Computer generated invoices and letterhead for many companies is commonplace these days. The majority of legitimate companies that use this form of correspondence tend to use preprinted stock, rather than generating the entire invoice or letter by using a printer. If a company is submitting invoices that look as though they may have come from a home computer, they may well have. This could be another warning sign that a fraud is in progress.[55]

Other Warning Signs

Investigators should also be alert to invoices that are submitted to a supervisor, rather than to an accounts payable department, or reception. This could be an indication that the supervisor is expecting the invoice and that it will receive an overriding approval since it likely doesn't have any proof of receipt to allow it to pass through the usual channels. This situation is even more suspicious when the invoices received directly by the supervisor are routinely for an amount just slightly below the supervisor's signing authority.[56]

Another common technique to have invoices processed without raising any warning signs is to try and use a name for the fictitious company that sounds and looks like the name of a legitimate vendor. For example, a supplier named "Built Right" may be used by a fictitious vendor scheme and changed to "Built Rite". This name will sound familiar to

---

[55] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 15.

[56] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 15.

anyone processing the invoices and may just make it through the accounting system without being detected as a fraud.[57]

Next Step: Electronic Detection

By taking a simple concept of looking for a specific set of evidence profiles in the records of a company as evidence that the risk of fraud has matured, and applying it to the various accounting streams within an organisation, we can perform consistent, complete, efficient searches in response to suspicions of fraud, or as a means of monitoring the accounting streams for these evidence profiles.

Once the risk of fraud has been identified, and the search for indicators of fraud begins, the process becomes more structured. The possibility of conducting at least some portion of this search electronically is real. The question becomes, "How far can electronic fraud detection go?"

The electronic data in an organization covers everything from the transactional data, to the copies of every e-mail message sent. This data represents a chronological account of everything that the company has done or been involved in. It follows that any event the company experiences will in some way manifest itself into this underlying chronology of events. In the event of a fraud, this manifestation is the evidence that investigators strive to uncover.

---

[57] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 16.

By taking an inductive approach to a fraud investigation, it's now possible to let computers search out the symptoms of fraud. Mr. Eckhardt Kriel, a Technology Security Risk Services specialist at Ernst & Yong, LLP in Toronto, states that a specific suite of data mining software has been adapted to sift through the enormous volume of data that companies generate each day, looking for evidence of fraud. This evidence could be a deficiency in an internal control, or a more elaborate profile of a matured fraud risk. By populating the software with many thousands of these profiles, the computer is equipped to compare the data to what it would expect to see if a fraud had taken place. This goes back to the premise that in order to find a fraud, you have to know what it looks like.

This approach is nothing new. It is founded on an inductive reasoning approach to fraud investigation. That is, the search for evidence to confirm or refute a prior hypothesis. The exciting aspect to automating the search process is that it gives investigators a chance to look at virtually every piece of data the company has stored for evidence of a fraud, as well as comparing search results to identify relationships among the data that may have otherwise gone unnoticed due to the sheer volume of records involved. Not only that, but data mining technology can handle massive volumes of data quickly and efficiently.

The automated approach to searching for indicators of fraud could still be performed after first applying the elements of the Fraud triangle in order to focus the investigation to the areas of the highest perceived risk. Alternatively, the electronic analysis could be performed without the benefit of first considering the relative risk of fraud occurring. According to Mr. Kriel, this is possible because of the ability to search all data in a relatively short period of time. In searching all data, the areas of high risk, as well as the

areas of low risk at the most fundamental level are all subjected to the same level of scrutiny, thus reducing the benefit derived from first identifying the relative fraud risk.

The result is that virtually all of the records of the company have been checked and crosschecked for signs of fraud. This is a very comprehensive approach that would not have been economically feasible only a few years ago. With the advances in software and hardware capabilities and in the reduction in the costs, this capability is now a reality.

Like any approach to a problem, there are some drawbacks. As with any red flag approach, the computer analysis will only identify the profiles that exist in the data that match the profiles that have been programmed into the data mining software, just as an investigator relying solely on a checklist will likely only ask the questions listed on the page. As discussed above, the number of potential fraud schemes is really limited only by the creativity and imagination of the fraudsters prepared to execute them. This makes the likelihood of programming data profiles to match all known and possible fraud schemes impossible. Current software can, however, "learn" from its mistakes. In fact, that was largely how it came to exist! By taking the profile of a fraud that was overlooked by previous electronic search process, and adding to the "checklist" programmed into the software, the search can actually get more thorough with experience – just as a fraud investigator gets more adept at locating evidence with experience.

This tool is currently being used to analyse the data in various data streams produced by routine business processes. Experience to date has shown that the processes in place over the payroll stream and the purchases, accounts payables, and payment stream are generally sufficiently similar in most companies to produce meaningful results from economically transportable profiles. Trials are currently being conducted on other

accounting streams, such as the revenue, accounts receivable, and receipts stream, the capital purchasing stream, and the inventory stream, that will allow the future development of industry-specific tools. These specialized versions will incorporate the same methodology for locating the evidence of fraud, but will be programmed to function effectively in the unique environments of various industries.

Once a tool like this makes the search for fraud efficient and effective, the possibilities abound. The tool could be run at any interval and on any business unit. If the process is truly streamlined, it would follow that the analysis should be done on a regular interval to allow a more prompt response to the evidence identified. If someone is embezzling millions of dollars from a company, why wait for twelve months to find out about it?

Such a process could be run annually as part of the typical year-end audit procedures, or it could be run quarterly to coincide with the release of internal quarterly financial statements. It may also be run only when someone suspects a problem. These alternatives all offer some different level of monitoring and various degrees of comfort. However, even after only a few months pass, the chance of recovering millions of dollars that have been wired from account to account, laundered and disbursed is greatly reduced. To minimise this exposure, Mr. Kriel suggests that the data-mining tool could be developed to run in the background of the corporate accounting and e-mail applications. This would provide real time monitoring of the transactions as they are entered into the systems. That is to say that if an entry was posted that fit the profile of a matured fraud risk, the transaction could immediately be brought to the attention of a supervisor, or investigation department for further analysis. This could cut the lead time

fraudsters currently enjoy from sometimes more than a year to mere hours, and greatly increase the chances of recovering the loss, or preventing the loss altogether.

A further advantage to having real time monitoring is that it effectively takes the detect role of a fraud investigation and turns it into a prevent control. This moves the nature of fraud risk monitoring from reactive, where an investigation is conducted after the company has been victimised, to proactive, where there is an ongoing search for indications that a fraud may be in the works. This switch could have a significant impact on the public's perception of the company, which would in turn have a positive impact on share prices, and on the employees' perception of the company. Indeed this could be a major influence on the corporate culture of the organisation. This one endeavour could positively impact employee morale as well as act as a deterrent to any would-be fraudster that were just waiting for the opportunity to present itself.

Current literature

Much of the current literature on fraud examines factors associated with frauds that have been discovered and documented. These studies tend to focus to a large degree on the effects on the company, such as monetary loss, employee morale and public perception.[58] These studies, though, do not address why and how long term, trusted employees can suddenly decide to commit a fraud against their employer and risk their career, their

---

[58] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 78.

reputation, and in some instances the respect of their family and friends. It appears as though the reason for this is that the victims of these frauds are reluctant to share the information with the public for fear of embarrassment, loss of public and employee confidence or a negative impact to their stock price. In the few cases that go before the courts the parties are often bound by confidentiality, so even when frauds are identified, there is usually little opportunity to learn from the mistakes of others.

While there are numerous textbooks and opinions as to the most effective techniques for fraud investigation, there is a definite lack of statistical research on how best to investigate a fraud. The statistics available are necessarily limited to those frauds that we know about. The total number of frauds that go undetected is a matter that is heavily debated, but impossible to prove.[59]

Because of these limitations in the current literature, behavioural research is becoming more and more important in learning how to investigate fraud more efficiently and more effectively.[60] One interesting observation is that there is a definite shift in current standards set by the AICPA. SAS no. 99 has adopted a focus much more aligned with the behaviour based fraud risk assessment, looking at motivation, opportunity and

---

[59] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research.* 4, 91.

[60] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research.* 4, 92.

rationalisation. The preceding guidance, SAS no. 82, by comparison appeared to be more of a reaction to a need for guidance, rather than true guidance. While the fraud indicator approach satisfied a need for some direction, the value of the guidance appears to be questionable.[61] Any subject that deals in part with human behaviour is bound to be dynamic and full of variables that interact in ways that are nearly impossible to explain. Therefore, addressing this subject, as SAS no. 82 did with fraud, with a static checklist approach was bound to be of limited value.

Another issue at hand is the underlying training received by fraud investigators. According to Dr. Philip Beaulieu, a Professor of Accounting at the University of Calgary, fraud is considered in many university business programs to be a by-product of business. There is little or no focus on what it is, how to prevent it, or how to find it. Practical training for fraud investigation comes only through very specialized programs, rather than recognising that fraud is now a very real part of business. It would appear that universities should be offering some advanced education on the impact of fraud at the levels of education where most future managers, executives and fraud investigators begin building their foundations. Planting the seed for fraud awareness at an earlier stage in someone's career would better prepare them to put their life's experience into this new context. Imagine gaining access to your ability to smell only after completing a university degree and articling with a company for three additional years. Not only

---

[61] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 83.

would you be overwhelmed with the new information you were receiving, but you wouldn't know how to effectively use this new sense with out a great deal of practice. You may not even be able to distinguish between bad smells and good smells.

Conclusions

It is a commonly held belief that the universe of fraud is composed of three categories. The first category is the fraud that has been prosecuted, and so is a matter of public record. The second category is the fraud that has been discovered, but that has not been prosecuted. This category results mostly because of investigations that are unable to turn up conclusive evidence as to the identity of the perpetrator or the extent of the fraud, and also because frequently instances of fraud are settled discreetly to avoid the associated embarrassment. The last category is the fraud that has not yet been discovered.[62]

There has been much speculation as to the relative size of these categories. We can only ever know with certainty the size of the first category. Based on this, we may speculate on the size of the second category, but we will never really have the answer to the size of the last category – or of the nature of this fraud. The fraud included in this last category could be similar to the fraud in the other two categories, and simply not yet discovered. Alternatively, the fraud in category three could be much more ominous – fraud unlike

---

[62] Davia, H., Coggins, P, Wideman, J., Kastantin, J. (2002). Accountant's Guide to Fraud Detection and Control, Second Edition, 2, 33.

anything contemplated or investigated to date.[63] One estimate of the relative sizes of these categories is 20 percent for category one, 40 percent for category two and 40% for category three. That means that for every fraud that is prosecuted, two instances of fraud go completely undiscovered – regardless of the approach implemented. Is this the result of highly intelligent fraudsters, or inadequate investigations?

It's clearly difficult to evaluate a process or methodology for detecting fraud. While you can monitor the number of frauds detected using a specific approach, you can never really be sure of the total population of frauds you are dealing with. Even when a fraud is successfully identified, how can you be sure that it wouldn't have come to light no matter what approach your investigation took?[64] Fraud's enduring pervasiveness, and continuing erosion of global economic and social development label fraud as a global socially intractable problem. It would seem that the general acceptance of the concept of the fraud triangle, and continued developments in technology offer the promise of investigative and risk management methodologies that combine behavioural science and data analytics into a comprehensive strategy to address the intractable qualities that have kept fraud on the agenda politicians and regulators around the world and raised its priority to unprecedented levels in the last year.

---

[63] Davia, H., Coggins, P, Wideman, J., Kastantin, J. (2002). Accountant's Guide to Fraud Detection and Control, Second Edition, 2, 34.

[64] Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 91.

Bibliography

Albrecht, C., & Albrecht, S. (2002) The Deductive Method of Fraud Detection. 2002 Symposium on Auditing Problems, University of Kansas.

Albrecht, W., Romney, M., Cherrington, D., Payne, I. & Roe, A. (1982). How to Detect and Prevent Business Fraud.

American Institute of Certified Public Accountants (1997). Statement on Auditing Standard No. 82: Consideration of Fraud in a Financial Statement Audit.

American Institute of Certified Public Accountants (1997). Statement on Auditing Standard No. 99: Consideration of Fraud in a Financial Statement Audit.

American Institute of Certified Public Accountants (2001). The CPA's Handbook of Fraud and Commercial Crime Prevention, Chapter 5.

Asare, S., & Wright, A. (2002) The Impact of Fraud Risk Assessments and a Standard Audit Program on the Planning of Fraud Detection Plans. 2002 Symposium on Auditing Problems, University of Kansas.

Bedard, J., Simnett, R., & DeVoe-Talluto, J. (2001). Auditors' Consideration of Fraud: How Behavioural Research can Address the Concerns of Standard Setters, *Advances in Accounting Behavioural Research*. 4, 77-99.

Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 9-17.

Balogna, J. (1993). Handbook on Corporate Fraud.

Canadian Institute of Chartered Accountants Handbook. (2002). Section 5135: Auditors' Responsibility to Consider Fraud and Error in an Audit of Financial Statements.

Canadian Institute of Chartered Accountants Handbook. (2002). Section 5136: (2002): Misstatements – Illegal Acts.

Davia, H. (2000). Fraud 101 – Techniques and Strategies for Detection.

Davia, H., Coggins, P, Wideman, J., Kastantin, J. (2002). Accountant's Guide to Fraud Detection and Control, 2, 33-45.

Ernst & Young LLP. (February 2003). Press Release: It's an Inside Job – Majority of Corporate Fraudsters on the Payroll, 1-2. Retrieved June 16, 2003 from www.ey.com/GLOBAL/content.nsf/Canada/Media_-_2003_-_Global_Fraud_Survey

Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 3-29.

Ernst & Young, LLP. (August 2002). Press Release: One in Five Canadians Say Fraud Occurs in Their Workplace, 1-3. Retrieved June 16, 2003 from www.ey.com/GLOBAL/content.nsf/Canada/Media_-_2002_-_Workplace_Fraud

Ernst & Young, LLP. (January 2003). Fraud: The Unmanaged Risk. 8th Global Survey, 2-12.

Fogarty, J. (2002). Financial Statement Fraud - Today's Challenges. 2002 Symposium on Auditing Problems, University of Kansas.

Greenspan, E. (October 2000). Defending the "F Word", 2-8.

Hodson, N. (1996, Summer). Lead Them Not Into Temptation. *IVEY Business Quarterly*, 1-5.

Landsittle, D. (2002). Detecting Financial Statement Fraud: Proposed SAS 82 Revision. 2002 Symposium on Auditing Problems, University of Kansas, 48.

META Group. (April 2003). Press Release: 80% of Users Prefer e-mail as Business Communication Tool, Says META Group, 1-3. Retrieved June 16, 2003 from domino.metagroup.com/pressHome.nsf/(webPressRelease)/D279165CF57E39878 5256D10004C9B41

Moyes, G. (1991). An Analysis of the Effectiveness of Specific Auditing Techniques for Detecting Fraud as Perceived by Three Different Auditors.

Ramos, M. (January 2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 28-36.

Wells, J. (March 2003). Protect Small Business. *Journal of Accountancy*, 26-32.

Young, M. (2002). Accounting Irregularities and Financial Fraud, Second Edition, 1, 1-21.

Zeir, J. (2001). The Expert Accountant in Civil Litigation, 6, 87-91

Appendix 1

Documents reviewed and Interviews conducted

This research paper was prepared based on interviews with the following people:

Dr. Philip R. Beaulieu, PhD, Professor of Accounting, Haskayne School of Business, University of Calgary.

Dr. J. Thomas Dalby, PhD, CPSYCH, Professor of Forensic Psychology, Neuropsychology, University of Calgary.

Mr. Eckhardt J.Kriel, CA, Principal, Technology Security Risk Services, Ernst & Young LLP, Toronto.

A detailed listing of the documents reviewed in researching this paper is contained in the bibliography.

Appendix 2

Sample Exposure Analysis

Appendix 1: Sample Exposure Analysis

This appendix contains an example of an exposure analysis used to capture the risk assessment in various areas of a typical retail organization. This example is not meant to be a comprehensive listing of all possible risk hypotheses, but rather is used to illustrate how the assessment of control in these various areas may take place.

The following table summarizes the risk assessments by location.

Summary

	High	Medium	Low	Total
Inventory/Shipping		1	1	**2**
Accounts Payable/Payments		3		**3**
Reception		1	2	**3**
Accounts Receivable/Sales			4	**4**
Capital Projects		1	1	**2**
	10	**23**	**35**	**68**

Inventory/Shipping

Risk Hypothesis	Prevent Control	Subvert	Detect Control	Subvert	Risk Assessment
Employee removes assets upon receipt prior to entry into inventory system.	Shipping and receiving area closed to all but essential staff.	Gain access to shipping area or partner with employee from shipping area	Receiving report generated and reconciled to invoice to ensure all goods shipped and invoiced are received.	Alter receiving report to indicate that entire shipment was received	Low – Subversion of the controls in place would entail collusion or
Employee removes assets from inventory	Access to inventory is restricted with physical security.	Individual would have to be assigned a key or obtain a key from someone else.	Inventory storage facility is monitored with security cameras. Inventory is reconciled to the perpetual records weekly.		Moderate – Theft from the inventory storage area is possible, but detection is likely, and occurs regularly.

Accounts Payable/Payments

Risk Hypothesis	Prevent Control	Subvert	Detect Control	Subvert	Risk Assessment
Employee submits invoice from fictitious supplier for payment	New vendors are pre-approved by accounting supervisor only. Cannot initiate a payment manually or electronically unless vendor is pre-approved.		Monthly disbursement summary shows payee on all cheques grouped by expense category and reviewed by accounting supervisor.		Low - Difficult to overcome controls.
Employee alters payee on cheque generated by AP department and negotiates cheque.	Signed cheques are copied by the receptionist and mailed immediately.	Receptionist would have to perpetrate the fraud	Unpaid vendor will contact accounting office to determine why payment not made.		Moderate – Detect control is very difficult to subvert.

Reception

Risk Hypothesis	Prevent Control	Subvert	Detect Control	Subvert	Risk Assessment
Cash received in mail is intercepted by receptionist prior to being entered into the accounting system.	Cash is not commonly sent for payment of outstanding invoices.		Account to which the cash should have been applied would age and ultimately be contacted to arrange payment.	Outstanding account receivable would have to be written off to avoid having customer contacted.	Low – Opportunity to commit these scenarios is low and detection risk is high.
Receptionist intercepts signed cheque to supplier, alters payee and negotiates personally.			Vendor would contact company for payment once account went unsettled for more than 60 days		Moderate – detect control difficult to subvert, but no prevent control. Opportunity is high.

Accounts Receivable/Receipts

Risk Hypothesis	Prevent Control	Subvert	Detect Control	Subvert	Risk Assessment
Employee intercepts funds prior to recording receipt in the accounting system and negotiates funds personally			Any funds received are logged in by the receptionist and a copy of the log goes to the accounting department with the funds. Account to which the funds were to be applied would age and ultimately be contacted to determine why payment was delinquent.		Low – Opportunity is low. Probability of detection is high. Difficult to negotiate cheque.
Cheque issued to employee of employee company and coded to account receivable for a customer and ultimately written	Accounting supervisor signs all cheques and would likely notice employee name.		Monthly disbursement summary by expense code would not reconcile, as disbursement would be made to an		Low – extremely difficult to have a new vendor added to the pre-approved vendor listing to enable payment to be made.

Risk Hypothesis	Prevent Control	Subvert	Detect Control	Subvert	Risk Assessment
off.	Cheque issued to vendor would have to be on the pre-approved vendor listing, set up by the accounting supervisor.		account receivable rather than an expense category.		Probability of detection is high.

Appendix 3

Sample Red Flag Checklist

Appendix 2: Sample Red Flag Checklist

The following 'Red Flags' are based on the information contained in reference sources from Banks (2001)[65], the AICPA (2001)[66] and Ernst & Young (2000)[67]. These fraud indicators are examples of indicators included in various checklists, and are not meant to be a complete list of fraud indicators.

People

- Management dominated by a single person or a small group at a senior level, with no accountability or oversight
- High turnover rate of personnel in key positions
- Long term employees with extensive knowledge of internal controls and year end audit process
- Understaffing of accounting and internal audit departments leading to reduced segregation of duties and reduced monitoring of controls
- Many or extensive changes of professional service providers such as auditors or law firms
- Unrealistic deadlines for financial reporting

---

[65] Banks, D. (2001). Auditing Accounts Payable for Fraud, 3, 9-17.

[66] American Institute of Certified Public Accountants (2001). The CPA's Handbook of Fraud and Commercial Crime Prevention, 5, 3-33.

[67] Ernst & Young, LLP. (April 2000). Fraud: Risk and Prevention, 28-29.

- Low employee morale
- Extensive overtime by one or a few key financial personnel
- Significant remuneration dependant on achieving loft or unrealistic performance goals
- An employee with a lifestyle that is inconsistent with their income, particularly if this has been a sudden, unexplained change

Processes

- A lack of screening for employees, such as checking references and for the existence of criminal records, particularly employees in key positions
- A lack of pre-approval for vendors or customers to ensure legitimacy, credit worthiness, relationships with employees. Also, no controls over adding vendors or customers to these lists if they exist
- Frequent transactions with customers or vendors that have bad business reputations
- Transactions with customers or suppliers that share mailing or contact information (address, phone, representative)
- High instance of management override of controls, or where management involvement is the only form of internal control
- History or suspicion of fraud that has not been investigated
- Little confidence placed on internal financial information
- Employee vacations not enforced, especially for key personnel

- Loss of financial records or untimely processing/reporting of financial information
- Complex reporting structure that is understood by only a select few of the organization's senior management
- Little time and resources devoted to planning and budgeting, and/or lack of monitoring of performance against plan or budget

Financial Results

- One or few unusual transactions that have a significant impact on the performance of the company, especially if the transactions are booked close to the end of the fiscal year
- One or few transactions, as above, that have the effect of raising the company results to a point that is just above the plan or budget, especially if this budget is significant for payment of performance based compensation
- Significant transactions with related parties, especially companies that are not commonly known to employees or auditors
- Financial results that are not consistent with other companies in the industry
- "Secret" transactions where customers will only deal with upper management or one employee
- Transactions based on unsigned contracts, or with unknown customers
- Cash flows not consistent with profits reported