Considering the Fraud Triangle in Compliance Risk Assessments

October 15, 2018

By: John Hanson, CPA, CFE, CCEP (*JHanson@ArtificeForensic.com*)

Forward

In the Spring of 2012 I published a five-part series of on-line articles through Corporate Compliance Insights under the heading of "*Incorporating the Fraud Triangle into Compliance Risk Assessments.*" While those articles were publicly available, I understand they received a fair degree of attention and were quoted and/or cited by numerous persons doing white-papers or articles where this information was relevant. A friend in the compliance profession recently told me that this series of articles was no longer available publicly/online and asked if I might consider updating/revising that work into one complete article and putting it back out into the public domain – here it is.

I believe the first time I was exposed to the Fraud Triangle was in 1990 or 1991 at an Association of Certified Fraud Examiners seminar in New Orleans. At that time, I was serving as the Director of Internal Audit and Quality Control for a privately held company. As the seminar facilitator explained the Fraud Triangle, bells and whistles began ringing loudly in my head about a particular person within my organization. This led to the first time that I uncovered an internal fraud.

In the nearly 30 years since then, I've accumulated a vast amount of experience investigating fraud, including almost a decade as an FBI Agent specializing in white collar crime (the FBI's term for "fraud"). I spent my last 18 months in the FBI as an Instructor at the FBI Academy, where, among other things, I taught "New Agents" how to incorporate the Fraud Triangle into their criminal fraud investigations. While many have attempted to expand or detract from the Fraud Triangle over the years, my experience has found it to be spot on. If I could supplement it in any way, it would only be the effect of the *perception of detection*, which I've incorporated into this article.

During my tenure in the FBI (1995 – 2004), corporate prosecution was not a "hot-topic." Agents were trained and charged with investigating individuals, not organizations. Even though the United States Federal Sentencing Guidelines ("FSG") detailed what it considered to be an effective Corporate Compliance and Ethics Program (hereafter "Program"), prosecutors weren't widely or actively pursuing organizations – unless, of course, they were a complete sham in the first place.

Then came along Enron and Arthur Andersen, circa 2001/2002. In some respects, those investigations and resulting prosecutions could be considered the womb that gave birth to the industry of corporate compliance and ethics. It was in the wake of the fall of these giants that prosecutors began to aggressively turn their sites towards organizations where misconduct had occurred, and it was very quickly appreciated by organizations and white-collar defense attorneys alike that, in accordance with the FSG, an organization's Program was the prime factor in determining corporate criminal liability by prosecutors. Since that time, other government agencies, as well as Suspension and Debarment Officials, have followed suit.

After leaving the FBI in late 2004, I took a leadership role in the forensic accounting practice of one of the large publicly-traded consulting firms, where for the next five and a half years I led investigations of corporate fraud and misconduct. It was in this context that I was first exposed to corporate compliance & ethics programs, which, as an industry and in terms of best practices, was still really in its infancy. My exposure was intensified in 2008, when I led a team appointed to serve as the Independent Corporate Monitor of a large publicly traded company. The primary focus of that Monitorship was the organization's overall Corporate Compliance and Ethics Program and I quickly realized that I needed to become an expert in this field.

I began consuming any information I could find about compliance and ethics programs and best practices, which immediately made me more effective in that Monitorship. In June 2008, I became a member of the Society of Corporate Compliance and Ethics and was certified as a Certified Compliance and Ethics Professional a few months later. I continued to not only study and learn about Programs, but experienced their best practices being put in place by the company I was monitoring through January 2010, at which point I left my role with the firm I was with (along with my leadership of that Monitorship) to start my own boutique consultancy.

Since that time, I have been directly appointed 4 times as a Monitor and have been engaged on 2 other occasions by Monitors. In all of these Monitorships, the primary scope and focus was the organization's overall corporate compliance and ethics program. During this same time, I've also continued to provide remedial recommendations to organizations concerning failures and/or weaknesses in their Programs that I identified in the course my internal investigations of misconduct.

Recently, I took on an engagement that has brought my compliance experience to a whole new level. I was engaged to serve as the Chief Compliance and Ethics Officer on an outsourced basis of a privately held 1,300+ employee company. In this role, I've had to design the Program from the ground up, then implement and maintain it. Despite all my experience in this field, I must admit it has been an eye-opening experience and one that has greatly improved my ability to more effectively (and efficiently) relate with and serve future clients. So, to all of my Compliance Officer friends out there, I can now state with no degree of uncertainty, "I feel your pain."

Whether serving as a Monitor, leading an internal investigation of potential misconduct, or now wearing the hat of a Chief Compliance Officer, I have found that incorporating the fraud triangle into various aspects of my compliance work has made me more effective. This article shares my thoughts on how compliance professionals, as well as consultants, can enhance the effectiveness of their compliance risk assessments by incorporating the Fraud Triangle into their work.

Overview

Assessing compliance risks is a fundamental and foundational part of an effective Program. Once the risks are identified, they are prioritized and addressed, often in accordance with a Board and/or Management approved Compliance Plan. This may include revising or drafting policies, conducting training sessions, and auditing/testing, among many other things.

While there are many effective ways to go about assessing compliance risks, compliance professionals might consider incorporating into their chosen assessment methodologies the Fraud Triangle, which may assist them in not only assessing risks, but also with prioritizing and addressing them.

The "Fraud Triangle" is a many decades old theory developed by Dr. Donald R. Cressey, a renowned sociologist and criminologist, that has withstood the test of time. It identifies three causal factors for occupational fraud. When the risks increase within all three factors, the risk of occupational fraud increases.

To better understand this, lets first distinguish "occupational fraud" from "predatory fraud"[1]:

> Occupational Fraud: "Internal" fraud that is committed by an executive, employee, or other agent of an organization who takes advantage of their employment or occupational position for their personal benefit by intentionally misusing, misapplying, or misappropriating an organization's assets and/or resources. For example, a CFO who embezzles company funds.
>
> Predatory Fraud: "External" fraud, commonly associated with "con-artists", professional fraud rings, or other organizational "outsiders" who devise schemes to deceive people or entities in order to enrich themselves or for other personal gain. For example, an offer from a Nigerian Official/Attorney promising you 10% of $40MM if you simply let them move those funds into your account.

[1] While the term "occupational fraud" appears to have been coined by the Association of Certified Fraud Examiners (Dr. Cressey's research was on embezzlers) and has become an accepted and common term in the fraud investigation community, the author coined and has been using the term "predatory fraud" for nearly 20 years when providing instruction on the Fraud Triangle in order to differentiate the types of fraud relevant to the Fraud Triangle.

Though Dr. Cressey's Fraud Triangle was concerned with criminal acts of fraud, particularly embezzlement, my experience has shown that his theory also applies to various forms of misconduct that may not arise to the level of criminal acts, such as violating a corporate compliance policy.

While organizations may certainly fall victim to predatory fraud, their greater risks may relate to their exposure to, among other things, criminal prosecution, suspension/debarment, de-listing, and/or civil liability associated with internal fraud or misconduct, in large part due to the vicarious liability that attaches to the organization for the acts of their employees, agents, etc. While predatory/external fraud can lead to significant organizational exposure, particularly if the company failed to adequately safeguard information, technology, or assets held in a fiduciary capacity, this article focuses on occupational/internal fraud or misconduct and/or non-compliance risks. Simply put, the Fraud Triangle was never intended and does not apply to "predatory fraud."

The Fraud Triangle

The three causal factors of the Fraud Triangle are: Opportunity, Rationalization, and Motivation.

Opportunity concerns a person's ability to commit fraud and is affected by such things as, among other things: internal controls, knowledge, training, education, authority, and experience. Though internal controls are a common and effective means of reducing the Opportunity factor's risks, persons with more than ordinary knowledge, training, education, authority, or experience may be better able to devise schemes to circumvent internal controls and/or conceal fraudulent acts.

For example, assuming internal controls are the same, a CFO who has a degree in accounting, is a CPA, and has been employed in that role for many years can better devise a scheme to circumvent controls than someone just out of college with a finance degree.

Rationalization concerns a person's ability to internally justify their wrongful actions. This is often affected not only by a person's individual moral compass, but also by the ethical tone within an organization and the person's perception about the fairness and equality of rewards and punishments for actions and behavior.

I was taught in the FBI that approximately 90% of human beings have a conscience (the other 10% are sociopaths).[2] For those of us in the majority, that means that when we do something wrong, it creates anxiety that we struggle with internally. Think back to when you were a child and you did something that you knew your

[2] I can't vouch for the accuracy of 10% and others disagree. For example, in Martha Stout's 2005 book "The Sociopath Next Door," she estimated that sociopaths make up 4% of the U.S. population. The actual percentage is irrelevant for these purposes – the only point is that almost everyone has a conscience and rationalization does not apply to those who don't.

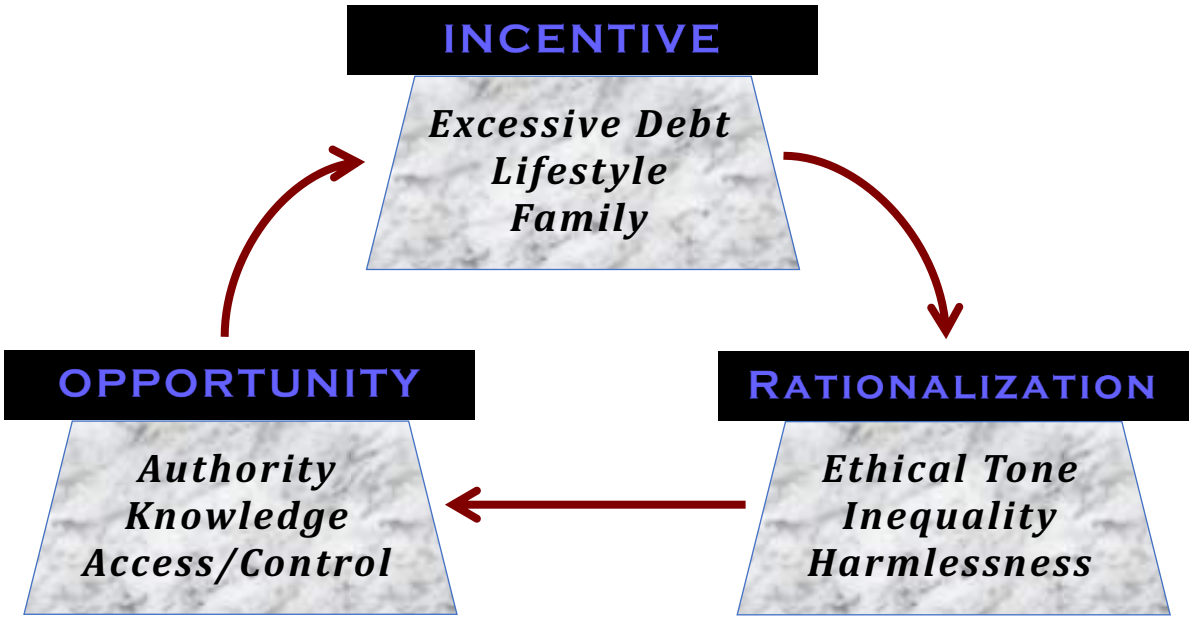
parents would not approve of – did your stomach turn on the inside a bit? In order for us to minimize that internal anxiety ("guilt"), we have to find a way to justify and/or rationalize it, lest it eat away at us (e.g. Edgar Allan Poe's "*The Tell-Tale Heart*").

I have seen this confirmed more times than I can count after taking confessions from people who committed fraud. In most instances and in despite of the consequences, they later told me that confessing their misconduct made them feel as though a great weight had been lifted from them.

Motivation, in the context of the Fraud Triangle, relates to a perceived "unshareable need" within a person's life. This need can arise from a broad range of things, from common and ordinary life issues to those that are more nefarious. For fraud, where the misconduct involves some action that results in financial gain, the motivation is that which drives the need for the financial gain.

For example, a person with a loved one dying from a terminal disease may need financial resources to care for that person, but for whatever reason, they perceive that they cannot ask their organization for financial assistance. On the more "nefarious" side, that financial need could be driven by a drug addiction, such that a person realizes that asking his/her organization for "$50 to get an eight-ball on the street to get high" would not likely be well received and may result in the termination of their employment.

The following helps illustrate the concept of the Fraud Triangle:



Though not technically part of the Fraud Triangle, there is another consideration that I believe is important as it relates to whether or not a person might commit fraud - the **perception** regarding whether or not they will get caught. In my experience, the perception of detection can be an overriding factor, such that even if the risks are high within the three causal Fraud Triangle factors, a person who perceives they will get caught will be less likely to violate a company policy, act unethically, or commit a fraud.

Opportunity

The most common means by which organizations can impact a person's opportunity to commit fraud, engage in misconduct, and/or deviate from company policies/procedures is through internal controls. Such controls may include segregation of duties, approvals, authority levels/restrictions, physical access, etc. An organization must balance the degree and level of internal controls with its associated risks and costs, such that the ideal system of controls intended to prevent fraud, misconduct, and/or policy deviations are more an aspiration than an actuality.

In performing a compliance risk assessment, the internal control system(s) must be understood and assessed. The degree to which internal controls help better reduce a person's opportunity to commit fraud, engage in misconduct, and/or violate company policies affects the associated compliance risk(s). Compliance Officers might consider consulting with Internal Audit, IT, Finance, and other departments as part of understanding and assessing the internal controls in place. For example, many organizations have policies that address gift giving/receiving by employees. In some instances, those organizations may have a significant degree of risk should such policies be violated (e.g. government contractors). If the system of internal controls related to the approval and reimbursements of employee expenses are strong, the associated risk of non-compliance might be reduced.

More importantly, internal controls are only as good as their application and adherence. I can't count how many times I have encountered an organization that had sound written internal controls, but they weren't understood, complied with, or enforced. For example, having a dedicated "vendor file master" (someone who sets up vendors and maintains the vendor file, but cannot approve invoices, issue payments, etc.) is an effective means of helping prevent many common Accounts Payable fraud schemes; however, if the person in that role (the "vendor file master") doesn't understand the importance of the role or adhere to the procedures in place surrounding the set-up and maintenance of the vendor file, that particular internal control fails. Interviews should include questions that probe the effectiveness of such controls, particularly if the person interviewed is in a "gatekeeper" type of role.

One question I have found helpful when interviewing such persons is: *"If you were to be promoted or leave the company and someone took over your role who lacked the same level of integrity that you have, how could that person violate a policy or steal and avoid detection?"*

The structuring of this question is intended to displace the interviewee from the misconduct, allowing him or her to provide a more genuine and honest response. I often find that I need to provide an example as well, to help the person apply their working knowledge and experience in thinking through the controls – and ways to get around them.

During one of my Monitorships, I once found during an interview that a supervisor simply scanned expense reports that he approved each month. He had a large number to review and approve each month and told me that he just didn't have time to look at them in detail and he trusted his subordinates. When I pointed out to him an expense that he had approved by one employee that clearly appeared not to be a company expense, he shrugged his shoulders. When I further pointed out that this expense was invoiced to the federal government and therefore created a potential criminal False Claims violation which may have to be reported under the FAR Mandatory Disclosure Act, he recognized the effect of his failure. He had not only failed to comply with the company's policy, but also failed in his gatekeeper role and allowed a fraud to occur.[3]

Also factoring into the Fraud Triangle's Opportunity factor is a person's knowledge, authority, and/or experience. Who is more likely to affect a greater fraud or more impactful compliance violation, a Chief Financial Officer or a line-level sales person? A new employee or one who has been in a particular role for many years? Clearly, those with more knowledge, authority, and/or experience can devise more ways to circumvent internal controls to commit larger frauds, along with better means to conceal them. In assessing the internal controls in place, the Compliance Officer should identify and be aware of such persons and pay particular attention to the internal controls relevant to them.

Consideration of the Fraud Triangle's Opportunity factor can help a Compliance Officer both identify and prioritize compliance risks. Audits and other techniques can then be accordingly planned to continuously monitor and report on such risks.

[3] The failure in this case was not just the supervisor not reviewing expense reports in accordance with his company's policies and procedures, but also in the company's training of supervisors about the importance of this function and potential ramifications if it failed. The company's Compliance Department also did not conduct audits of expense reports, which was another failure in light of the compliance risk(s) associated with expense reports for government contractors.

Rationalization

Recall that in the context of the Fraud Triangle, Rationalization relates to a person's ability to internally justify their unethical, wrongful, or criminal actions and/or misconduct. This is often affected not only by a person's individual moral compass, but also by the ethical tone within an organization and the person's perception(s) about the fairness and equality of rewards and punishments for actions and behavior.

Among the chief elements of proving fraud are proving "knowledge" and "intent." Fraud is not a mistake. Neither is misconduct, ethical violations, and generally, though not necessarily, many compliance violations, though it is possible for a person to violate a compliance policy without realizing they have done so, particularly when the violation does not compromise ethical values and where no, little, and/or poor training has occurred to make the person aware of the compliance policies.

When one commits fraud, engages in misconduct, or acts unethically, he or she knows that they have done something wrong. With the exception of sociopaths, most people have a conscience and are "good," such that the temptation to do something wrong is affected by the anxiety that wrong-doing creates inside of them. Rationalization helps a person avoid or reduce that anxiety, enabling them to justify wrongful actions or behavior. Within an organization, rationalization is affected by such factors as, among others: ethical tone ("tone at the top"); fair and equal punishments for bad behavior or wrongful actions; decentralization; employee turnover; compensation; and career, promotional or award considerations.

An ethical tone that promotes high ethical values and standards, as well as good behavior and actions, can encourage good behavior and help reduce an employee's ability to rationalize actions inconsistent with that tone. If management condones or demonstrates a poor ethical tone, it increases the ability for employees to rationalize their own misconduct, perhaps even encourages them to do so (e.g. Bernie Madoff). Conversely, if management, starting at the highest level(s), promotes and demonstrates a high ethical tone, it is like an anti-virus that spreads throughout an organization.

Accordingly, Compliance Officers should incorporate an Ethical Tone Assessment into their Compliance Risk(s) Assessments. Understanding the ethical tone, real and perceived, will help the Compliance Officer evaluate the associated risk for the Rationalization factor of the Fraud Triangle, which directly relates to the compliance risk(s). In recent years, I have seen a trend in corporate settlement agreements with government agencies (i.e. deferred prosecution agreement, non-prosecution agreement, administrative agreements, etc.) requiring that the offending companies and/or their Corporate Monitor include ethical tone assessments in their work, indicating that government agencies have recognized the important role of ethical tone in preventing misconduct.

One of the most effective tools I have found in assessing ethical tone is interviews. Following are some example questions that I have found useful in helping me assess ethical tone, among other things:

- *"What should happen to someone who violates your company's Code of Conduct or Compliance Policies?"* - This is a modified "behavioral analysis" question. The purpose of the question is to assess the ethical tone of both the individual and the organization. Generally speaking, the appropriate response should be that those who violate the company's Code of Conduct or Compliance Policies should be fired and, if their actions broke the law, criminally prosecuted. While employees may vary in the severity of the punishments they believe appropriate, a pattern of responses that overly minimizes punishments may be indicative of an ethical tone that is not consistent with the company's expectations or desires.
- *"Are you aware of anyone who has not complied with or is not complying with your company's Code of Conduct or Compliance Policies?"* – If a pattern emerges where people identify either specific persons or levels of management where this is occurring, it could be indicative of an ethical tone concern. Additionally, this question also helps a Compliance Officer with other standard Compliance Program requirements: (1) it can be directly associated with the Compliance Officer's "monitoring" efforts to detect potential criminal conduct as per §8B2.1(5) (A) of the FSG and (2) it can also test compliance by managers and supervisors with internal policies requiring that any complaints from employees concerning compliance or ethics violations be reported to the Compliance Officer.
- *"What are the compliance and/or ethical challenges you face most frequently in your current role?"* - This question provides information on several important aspects of a Compliance Program:
    - It may uncover ethical challenges that directly relate to tone at the top and ethical tone.
    - It may identify risks that the Compliance Officer was unaware of or didn't fully appreciate in the risk assessment process.
    - It assesses how well employees are able to apply corporate policies in the context of their role (policy comprehension/retention and training effectiveness).
    - It reiterates and reinforces the employee's understanding of risks and policies specific to them (Training).

  I have found that interviewees frequently initially struggle with the last question and the interviewer may need to provide an obvious and relevant example of such a challenge to help the interviewee feel comfortable sharing this information. Starting with a policy that is relevant to most employees, such as a Gift Policy, can help open the conversation.

Another aspect of Rationalization concerns the perception regarding fair and equal punishments for bad behavior or wrongful actions. If Executives and/or senior people within organizations are perceived to be treated more leniently for ethics or compliance violations, those at lower levels are more able to rationalize their own violations. Organizations should strive to assure that their penalties for such violations are commensurate with the violation and that the penalties are applied equally to all within the organization, regardless of their position, role, or tenure.

It could also be argued that those at higher levels within organizations should be held to an even higher standard, given the impact upon the organization should they violate a compliance policy or act unethically. Such things as "golden parachutes" for Executives who leave their position, even if they left under circumstances involving misconduct and/or ethical or compliance violations, can increase an employee's ability to rationalize his or her own misconduct.

Compensation, along with career advancement/promotion opportunities and award considerations (e.g. bonuses) also affect the Rationalization factor of the Fraud Triangle. Such things should be based on merit and within some boundaries of equality and fairness. While Executives may often merit large bonuses and/or incentive-based compensation, taking such actions without the general employee population understanding the basis for it having been earned can engender an "us versus them" mentality within an organization that increases an employee's ability to rationalize misconduct.

While compensation cannot satisfy everyone's perception about their personal worth (most feel they are worth more than they are paid), a perception about compensation being fair helps mitigate the negative perceptions. In tough economic times, where many have not received raises, received minimal wages, and/or not been paid bonuses, organizations should consider the effect of rewarding only top-level persons and how such actions impact the Rationalization factor of the Fraud Triangle.

Similarly, when employees who have been in a position for some length of time are not promoted as others above them retire or are promoted themselves, it can affect the Rationalization factor. I once had an investigation where an Assistant Controller, despite many years of what she called "faithful service," was not promoted to Controller when that position was vacated. The company instead hired a relative of one of its Senior Management Team, who was young and inexperienced, to take the Controller position. The Assistant Controller felt that person had "taken her job" and used that to help rationalize an embezzlement scheme.

While hiring and promotion decisions should be done in accordance with the best interests of the organization, consideration should be given to how such decisions affect the Rationalization factor of the Fraud Triangle. An organization that routinely fills vacated positions from the outside rather than promoting from within may create an environment that better enables employees to rationalize misconduct. This should also be considered in light of the Opportunity factor of the Fraud Triangle. The more likely that those in positions that have greater opportunity for wrongdoing can rationalize such wrongdoing, the greater the risk that they might do so because two of the three factors of the Fraud Triangle are affected.

Any situations that create a more "individualistic," rather than a "team" or "corporate" environment can increase the risk of rationalization among employees as well. Decentralization, which can distance employees from the organization, as well as high-employee turnover, are two such areas that organizations frequently face. Another, which occurs frequently within organizations heavily involved in government contracting, is where employees are "inherited" from the previous government contractor, such that they may not appreciate or feel part of the organization that actually signs their paychecks.

Consideration of the Fraud Triangle's Rationalization factor can help a Compliance Officer both identify and prioritize compliance risks. In some instances, actions can be taken at a policy or policy enforcement level to help mitigate such risks. Audits can also be accordingly designed to continuously monitor and report on such risks.

Motivation

In the context of the Fraud Triangle, Motivation relates to a perceived "unshareable need" that arises within a person's life. It is the one area of the Fraud Triangle that an organization has the least control over, as well as the most difficult for a Compliance Officer to assess. This "unshareable need" is a personal need that can arise from a broad range of things ranging from common and ordinary life issues to those that are perceived as less publicly acceptable. As that need increases within a person's life, so too does the risk of that person acting contrary to an organization's Code of Conduct and/or Compliance Policies.

The difficulty with the Motivation factor of the Fraud Triangle results from the need most often being one that is perceived by the employee as "unshareable." For example, while most would expect that a person addicted to crack cocaine might not be inclined to share with their employer their financial need to support that addiction, many don't consider that an employee who is going through a nasty and expensive divorce might feel just as uncomfortable sharing their financial need(s), possibly perceiving that doing so might have a negative impact either on their career or their reputation.

Even such things as a change in mortgage terms (i.e. the conversion of a low interest/short term mortgage into a high interest/long term mortgage without an ability to re-finance) can be something that might cause personal embarrassment and prevent a person from sharing with their employer their financial hardship and situation.

As a former FBI Agent, FBI Academy White Collar Crime Instructor, professional fraud investigator, and Independent Corporate Monitor, I have seen all sorts of different needs that have motivated people to commit fraud, engage in misconduct, and/or violate compliance and ethics policies. Below is a small sampling of real-life examples that I have personally experienced (caution: life is stranger than fiction):

- Corporate Controller having an extra-marital affair
- Accounts Payable employee with a sick mother who could not afford treatments and medicine
- Sales Representative suffering from HIV/AIDS
- Divisional Manager with a gambling addiction
- Project Manager who wanted to "keep up with the Jones" in his social circles
- Salesperson who became addicted to heroin after sustaining a back injury
- CEO who fell victim to a Ponzi Scheme
- Account Representative whose mortgage terms changed
- Business Owner who fell victim to an Advanced Fee Scheme (the notorious "Nigerian Letters")
- Chief Operating Officer being "blackmailed" by a "Madame" (prostitution ring)
- Accounting/Finance employee whose son was going through gender transition treatments

The more an organization encourages and enables its employees to share what they otherwise might consider "unshareable," the better the Motivation factor of the Fraud Triangle can be assessed and addressed. For example, many organizations have employee assistance programs (EAPs), which encourage and enable employees to get assistance with personal needs. Such programs can directly impact the Motivation risk, to the extent that they are trusted (as to not impacting careers or creating social stigmas), easily available, confidential, and effective in addressing the employee's problems. For example, during the "mortgage crisis," some organizations directly provided or arranged for financing that could assist affected employees.

Depending on local, state and federal laws, as well as an organization's policies, internet and/or email usage might be monitored, which could bring red flags associated with some of the issues that can affect a person's Motivation to the organization's attention. For example, key word searches applied to work-related emails, such as "betting" or "overdue," may return relevant information about a person's unshareable needs that could impact that person's risk for misconduct as per the Fraud Triangle. This is obviously a very sensitive area and much consultation should be made with legal counsel before taking such actions.

Another way that the Motivation factor can be assessed/monitored is for those with supervisory responsibilities to receive training on the Fraud Triangle. Supervisors are closer to and should be more attuned to what is happening in the lives of their subordinates, such that they might become aware of potential personal problems or issues before they become a more serious problem. This is not "spying" on employees (which I don't condone), rather raising supervisory awareness to why people commit fraud in order to help the organization address the risk(s) timely and appropriately.

Compliance Officers might also consider spending more time with and getting to know employees. One of the first frauds I ever discovered was in the early 1990s, when I was Director of Internal Audit & Quality Control for a company. Though my position was considered an "Executive" within the company, I regularly ate in the lunchroom and socialized with company employees at all levels. That regular interaction made me more aware of what was happening in the personal lives of the company's employees, as well as what gossip was circulating around the company.

One day, while eating lunch with several employees, I heard that a lower-level employee had recently purchased a new and very expensive sports car. People were wondering how this person afforded the car and the scene from Superman III when Richard Pryor pulled into his company's parking lot in a Ferrari popped into my head (he bought the Ferrari using funds he stole from the company). I did a little digging and uncovered a possible kickback scheme involving this employee and a subcontractor.

For Compliance Officers conducting Compliance Risk Assessments, assessing the Motivation factor of the Fraud Triangle in the broad sense is the most difficult and non-direct of the three Fraud Triangle factors. Things to consider might include the existence and use of an EAP Program, availability of other "help" programs, and current economic trends and factors that might cause personal problems.

Compliance Officers should also more closely consider the Motivation factor in conjunction with the other Fraud Triangle factors they work into their Compliance Risk Assessment(s). If based upon an assessment that the risks associated with the Rationalization and Opportunity factors is particularly high for a particular group or role(s) within an organization, the Compliance Officer might then consider and assess Motivation more particular to those groups or roles at risks. Generally speaking, if the Opportunity and Rationalization risk factors are high, the overall risk for misconduct should be assessed as high, regardless of Motivation, which can be difficult or impossible to assess due to its very personal, dynamic, and "unshareable" nature. In the absence of an ability to assess Motivation, a Compliance Officer may elect to apply more focused and/or detailed audits of those areas.

Consideration of the Fraud Triangle's Motivation factor can also be useful in helping a Compliance Officer prioritize already identified compliance risks. As noted above, for those compliance risks where the Fraud Triangle's Opportunity and Rationalization risks are determined to be high, consideration of the Motivation factor may help the Compliance Officer further evaluate and prioritize those risks. The Compliance Officer can then determine the appropriate actions necessary to mitigate and address those compliance risks through the organization's Compliance and Ethics Program.

Perception of Detection

I have found that when a person perceives their misconduct will likely be detected, it influences their actions. So much so that it could be considered an "overriding factor" to the Fraud Triangle. In other words, even if the risks are high within the three Fraud Triangle factors, a person who perceives they will get caught will be less likely to violate a company policy, act unethically, engage in misconduct, or commit a fraud.

In this context, perception relates to the perception by an individual that their misconduct will be detected. The perception of detection may weigh more heavily on a person's decision than the punishment.[4] The reality of detection need not be consistent with the person's perception of detection, but the punishment(s) for those who are caught must be real – and known. Meaning if someone is caught for some form of misconduct, they must know that they will be punished for their actions, irrespective of tenure, position, title, rank, etc..

[4] Though one may find many articles and studies on this topic, among the foundational works is "An Introduction to the Principles of Morals and Legislation" by Jeremy Bentham (1789). It's not light reading, but well worth the time.

When the perception that misconduct will be detected is increased, it impacts behavior. A classic example is where non-active surveillance cameras are placed in areas where employees work, such as over checkout or bank teller counters. Even when those cameras are not active, the perception that they are active decreases the likelihood of theft in those locations.

Similarly, those who perceive that reconciliations or audits are routinely done and effective in detecting misconduct are less likely to do something wrong in the areas they perceive as being "monitored." While reconciliations and audits are key internal controls affecting the Opportunity factor of the Fraud Triangle, their impact on the Opportunity factor is dependent upon their actual and effective occurrence. For purposes of the perception of detection, those reconciliations and audits need not actually be occurring or effective, only perceived to be. As a preventative measure, it has the same effect. It is only in the detection of compliance deviations and/or misconduct where the mere perception fails.

According to the 2018 Association of Certified Fraud Examiners "Report to the Nations on Occupational Fraud and Abuse," most frauds are detected by tips.[5] The majority of those tips came from other employees, but they also came from vendors, customers, competitors and/or other "outside" parties. Many companies make available hotlines, which they publicize not only to employees, but also to other outside parties of concern. These hotlines can be used to anonymously report compliance violations, ethical misconduct and/or illegal activities. Given that tips play so prominently in detecting misconduct, Compliance Officers may consider how they could perpetuate and/or increase the perception of a hotline's effectiveness to employees.

In assessing (and promoting) the perception within an organization that misconduct will be detected, a Compliance Officer may consider the following:

- How well known and used is the organization's Hotline?
- Is the Hotline well publicized internally and externally (e.g. to relevant third-parties such as vendors, suppliers, customers, etc.)?
- Do employees believe that effective audits are routinely conducted?
- Do employees believe that reconciliations and inventory counts are effectively and routinely conducted?
- Do employees perceive that physical security measures (i.e. cameras, access cards, etc.) exist and are effective?
- Do employees know that the Compliance Officer conducts routine audits and monitoring and believe it to be effective?

[5] Association of Certified Fraud Examiners, "Report to the Nations – 2018 Global Study on Occupational Fraud and Abuse" (page 17).

- Do employees know and believe that the organization monitors corporate internet and email usage?
- Are employees made aware of instances where someone has been caught for violating a compliance policy, acting unethically and/or committing a fraud and how they were caught?

One effective tool that a Compliance Officer can use in assessing the perception of detection is interviews. Questions can be incorporated into a Compliance Officer's routine interviews that are designed to both gather the relevant information necessary for the assessment of this perception, as well as perpetuate and increase the perception about misconduct being detected. For example:

> *"As you know, we routinely conduct discreet audits of employee expenses designed specifically to identify policy violations and misconduct. Can you think of other ways that we might identify violations of our expense policy and/or misconduct?"*

This question immediately leads the employee to believe that such audits are occurring (and I hope they are), creating a perception that expense policy violations and/or misconduct have a greater likelihood of detection. It also may give the person cause to wonder what other audits might be taking place, increasing the person's perception about detection in other areas. This question also elicits the person's thoughts about potential work-arounds or circumventions of internal controls about which the interviewer may not have been aware, furthering the assessment of the Opportunity factor of the Fraud Triangle.

The Compliance Officer may also evaluate how well publicized, and to whom, the organization's hotline is. Is the hotline receiving any calls? From whom? What were the nature of the calls? The more the hotline is known, accessible, and used, the greater will be the perception that misconduct will be detected. If the Compliance Officer finds that the hotline is not well communicated, never called, and hard to find the number for, he or she can be assured that employees don't perceive it to be effective in detecting misconduct.

Another means of facilitating a greater degree of the perception of detection is to institute a "Duty to Report" policy that requires employees to report misconduct. If it is found that someone knew about misconduct and did not report it, that person subjects him or herself to disciplinary action, up to and including termination of employment. This is not intended to create a "snitch" environment, but rather to promote the reporting of misconduct and increase the perception of misconduct being reported (therefore "detected').

For organizations that have internal auditors, the Compliance Officer may consider the extent to which internal audit publicizes their yearly audit plans and their history of completing those plans. Though it is common that internal audit, for many reasonable and ordinary reasons, may not complete everything in their audit plan during a year, it is also common that not everyone knows it. To the extent that such audit plans are tied to risks, are conducted effectively, and believed to be occurring, the perception of their effectiveness in detecting misconduct is increased.

The same holds true for internal controls. Though internal controls are most often associated with the Opportunity factor of the Fraud Triangle, even when such controls are lacking or poorly administered, if they are perceived to be present and effective, the perception of detection is increased. For example, if supervisors are required to check and approve time sheets and perceived to be doing so effectively (even when they fail to do so), the perception that falsifying time sheets will be detected is increased, reducing the perception that one can do so and get away with it. This particular example also applies well with subcontractors!

Similar to Internal Audit, does the Compliance Officer make known his or her compliance audits and monitoring plans? While "unannounced audits," if used as a tool by the Compliance Officer would not be made known, making employees aware of what the Compliance Officer will be auditing and monitoring increases the perception that wrongdoing will be detected. To the extent that the Compliance Officer is not able to complete all of the audits and monitoring planned at the beginning of a yearly cycle, anything not done should be carried over and prioritized in the next yearly cycle, less the perception be created that Compliance Audits are a mere show.

The perception of detection has a significant impact. These are a few ideas about how Compliance Officers can assess and use this perception to their organization's advantage. Recognizing the impact of the perception of detection, along with understanding how such perceptions are created and promulgated, can be an effective tool for a Compliance Officer, both in evaluating risk(s) and in administering an effective Corporate Compliance & Ethics Program.