The GRC webinar series includes two separate segments that relate to the topic of Fraud. Segment 13 was on Fraud Awareness. The article that accompanies that segment poses a hypothetical scenario of an entrepreneur who starts his own business. The gentleman experiences some difficult struggles when he is required to entrust his carefully built business to others. In the end, he learns the importance of fraud awareness even when you do your best to hire honest, trustworthy personnel.

Fraud awareness techniques are unquestionably important concepts in today’s business world. Informing your employee base about fraud red flags in their processes, compliant procedures, and monitoring procedures should be considered a pro-active step in a company’s fraud monitoring program. I’ve heard individuals say that their senior management doesn’t believe in fraud awareness because they believe it is like teaching your employees
how to commit fraud. In my view, this thought process is very far from the truth and a bit in the dark ages. However, even if your company doesn’t engage in active fraud awareness techniques, it is imperative that some level of monitoring be employed to ensure the company is well protected.

Think of it this way, we teach our children to look both ways before crossing the street. They are told that this action is very important each and every time they cross the street. We do this to keep them safe and to teach them the importance of safety. But we all know that if we are not consistently monitoring or observing the behavior of our children each time they cross the street, there is a likely chance this important concept we’ve taught them may be forgotten when their favorite ball goes rolling down the road uncontrollably. We’ve made them aware of the concept and that it definitely important. But if we don’t periodically monitor their actions and observe what situations they may find themselves in, how do we appropriately correct their behavior in those instances when the hard taught lesson is forgotten?

Similarly, all the fraud awareness efforts we may put forth to teach our employees about why fraud happens, how it can happen, things to look for, the company’s stance on fraud and fraud evaluations need to be supported by adequate monitoring techniques. That isn’t to say we don’t trust our employees or we are trying to catch them in the act, it simply means that what is not monitored may not be effectively managed.

Ok, so we get it, fraud monitoring is something all companies should do. But how, when, where, who and what should be monitored? Those are all great questions and not one that can be answered the same way for every company. I bet you can guess what the next comment is, perform a fraud risk assessment.

As accountants and auditors we love the word assessment. We find ourselves using in in multiple ways including risk assessment, control environment assessment, accounting risk assessment, management assessment fraud risk assessment. The list is almost never ending. But we use the term assessment for good reasons. If we are going to be able to appropriately evaluate our processes and allocate scarce resources to perform certain responsibilities, it is incumbent upon us to ensure we adequately assess the probability that control gaps could manifest themselves in potential exposure to vulnerability. Many people will refer to monitoring travel and entertainment expenditures for inappropriate transactions. They correlate this to fraud monitoring. This certainly is an area that is available to monitoring procedures. But rationally thinking about it, if you are doing proper fraud awareness training and managers understand the company’s policies related to T&E, and you have a strong workflow process for expenditure submission and approval, is this highest priority area to allocate resources to for ongoing fraud monitoring? The answer could be yes, no and maybe and is very much dependent on your industry, regulatory requirements and the wishes of your Board. This example is exactly why it is important to do a complete fraud risk assessment and obtain management input and approval on the observations from that assessment.

It is important to recognize that to perform an effective fraud risk assessment, we must understand the root causes of misconduct. Through this understanding, you can focus on those processes in your organization that may be susceptible to exposures. For instance, in a survey by KPMG of over 5000 working audits, following are some statistics on the root cause of perceived misconduct:

- In 59% of cases perpetrators felt they needed to do whatever it takes to meet business goals.
- In 52% of cases, the perpetrator believed he would be rewarded for results, not means.
- In 51% of the cases, perpetrators didn’t believe the company took the code of conduct seriously.

Now, considering those facts, how would they come into play within your fraud risk assessment? Ask yourself a few questions:

- What process areas are under extreme pressures to meet business goals?
- Are there process areas that are expected to be the top performers year after year?
- What process areas have struggled with their earnings or profit targets?
- Are their instances that you can identify where an alleged misconduct occurred but it was downplayed because the results were acceptable to the organization?
What are the highest risk areas in your business that if the code of conduct is not taken seriously, their actions could have a dramatic impact on the organization? (E.g. Sales department, procurement department etc.)

The answers to the above questions could be very different from organization to organization or industry to industry. That is why there is not a one size fits all risk assessment process.

The point of the above exercise is to assist you in identifying what are the highest risk areas or most susceptible processes to the potential of fraud. In addition, if a fraud occurred in a specific area, how would it impact your organization? Remember, you can’t just think in financial terms. You must consider reputation, operations, corporate culture etc. An identified relatively small act of misconduct by a senior officer on their personal expense report that goes unaddressed could send very loud messages to the rest of the company and result in many unwanted repercussions. That is why many organizations have regular reviews of executive expenditure reports.

Besides understanding the root causes of misconduct, it is important to be aware of the components of the fraud triangle. But beyond that awareness, you must be able to relay the triangle component to situations that may exist in your organization. This exercise will assist in further identifying those areas that may be the most beneficial to monitor. First, let’s look at the fraud triangle itself.

The three primary components that experts claim must exist for fraud to occur are rationalization (they owe it to me), pressure (I might lose my job) and opportunity (lax or ineffective controls). How might these three elements provide you with insight into specific monitoring areas for fraud potential?

As a long-time auditor, I would most likely first point to opportunity. When controls are lax, ineffective or non-existent, then the probability that something will occur outside management expectations becomes greater. This is often the auditor’s dilemma. When performing an audit, we point out control gaps. But management likes to respond with so what, it is not a big deal! Well, maybe it is and maybe it isn’t. Management must recognize that the point of control assessment is not to prove the control break has created a financial exposure. Instead, it is an attempt to assist the organization in preventing potential exposures or possibly examine large transactions that may have been impacted by the control gap. With this in mind, a strong consideration in your fraud risk assessment process may be questions like:

* Which areas continue to experience control deficiencies?
* Where in the organization are changes prevalent and ongoing?
* Are there areas that appear resistant to control suggestions?
* Are there “off limits” areas in the business for internal audit?

These are just a few questions related to opportunity. You must also remember that the profile of the typical white collar fraudster is a long-term employee, trusted and well liked. That in itself creates opportunity. Of course, in determining monitoring areas for focus, we can’t forget the other two parts of the fraud triangle rationalization and pressure. Rationalization may very much be tied to individual traits which can be more difficult to assess. However, pressure can create rationalization so possibly consider what areas of your business have been under particular scrutiny for results. This may create the potential for inappropriate behavior.
Once you are able to adequately develop your fraud risk assessment, what next? First, you might consider what monitoring processes should be put in place within the organization to help support the overall control environment. These may be things such as employee background screenings, a whistleblower hotline, due diligence procedures on vendors, code of conduct acknowledgement, conflict of interest statements etc. These are the types of typical monitoring processes that advance your fraud awareness stance as well as ensure professionals understand that there are procedures in place to monitor activity. The next step should relate to prioritization of the more detailed results from your fraud risk assessment. Within the assessment, hopefully you have identified those areas where the act of misconduct is not only more likely to occur but also have an unacceptable impact on the organization. Once this is completed, first look to what checks and balances can be put in place to solidify the controls in the process area and allow management to monitor their individual processes. The first line of defense should be management. Then, past solidifying your control processes, you can begin to consider if there are other analytical procedures, audits or internal reviews that should be performed periodically to adequately monitor for the potential for fraud.

This thought brings up the topic of whose responsibility is it to monitor for fraud in the organization? The reality is fraud monitoring techniques should be a shared responsibility between management, the board, internal audit and external audit. The caution here is: don’t wait till the auditor’s show up. By that time, it may be too late. Most fraud studies show that a typical fraud may go 18-24 months before being detected. That would indicate that actions by management are critical in fraud prevention and probably are the first line of defense for fraud monitoring.

In summary, monitoring can be developed for almost any specific process. Management must consider what areas their organization may be most vulnerable to fraud. Monitoring techniques are management’s responsibility, not the auditors. Although both internal and external audit can assist in monitoring techniques, if you wait till the auditors arrive, you could be too late.