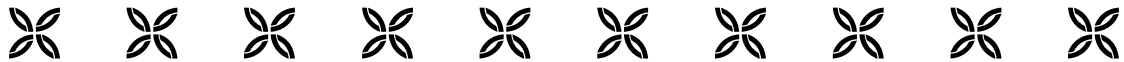


SUPPLY CHAIN FRAUD



An overview of a growing internal & external threat to the well-being of an organization.

Norman A. Katz, CFE, Katzscan Inc.



TABLE OF CONTENTS

INTRODUCTION2
RELATIONSHIP TO SARBANES-OXLEY3
COSO – SARBOX – SUPPLY CHAIN FRAUD4
DEFINITION: SUPPLY CHAIN5
DEFINITION: FRAUD6
WHO’S INVOLVED?7
WHAT CAUSES FRAUD?8
WHERE IT HAPPENS9
SUPPLY CHAIN FRAUDS10
IMPACTS OF SUPPLY CHAIN FRAUD11
SUPPLY CHAIN FRAUD DETECTION12
SHRINKAGE: BOTTEMLESS PIT OR GRAVE?13
ASSESS BEFORE THE AUDIT14
ARE YOU BUDGETED FOR FRAUD REPERCUSSIONS?15
SUMMARY16
ABOUT THE AUTHOR16
ABOUT THE COMPANY16

Is there fraud in your supply chain?

If so, how would you know?

INTRODUCTION

Few terms resonate so deeply with business these days as do “supply chain” and “fraud”. Individually, these two terms are a reflection of the evolving business world around us: the supply chain is truly global in nature, and it seems that fraud is being committed in both the public and private sector at alarming rates and dollar amounts, with more clever and audacious schemes being hatched on a regular basis.

Together though, the term “supply chain fraud” encompasses a growing (and possibly silent?) threat that strikes both wide and deep at an organization’s operations along the internal and external supply chain. The ramifications of fraud early in the supply chain may have significant impacts later on in the supply chain; yet to the untrained observer, the two instances of fraud may seem unrelated. Worse, the solution to reduce fraud may not cover all areas where fraud has occurred or the effects of fraud felt.

For turnaround professionals, auditors, fraud examiners and the like, as well as executive management and all levels of employee, understanding the depth and breadth of supply chain fraud is indeed crucial to helping ensure healthy organizations stay healthy, and helping distressed organizations become healthy again.

This white paper will provide the reader a comprehensive overview of what supply chain fraud encompasses, who the likely perpetrators are, where it is likely to be found, and what can be done to detect and reduce it, along with the relationship to Sarbanes-Oxley compliance, and with useful definitions of the “supply chain” and of “fraud”.

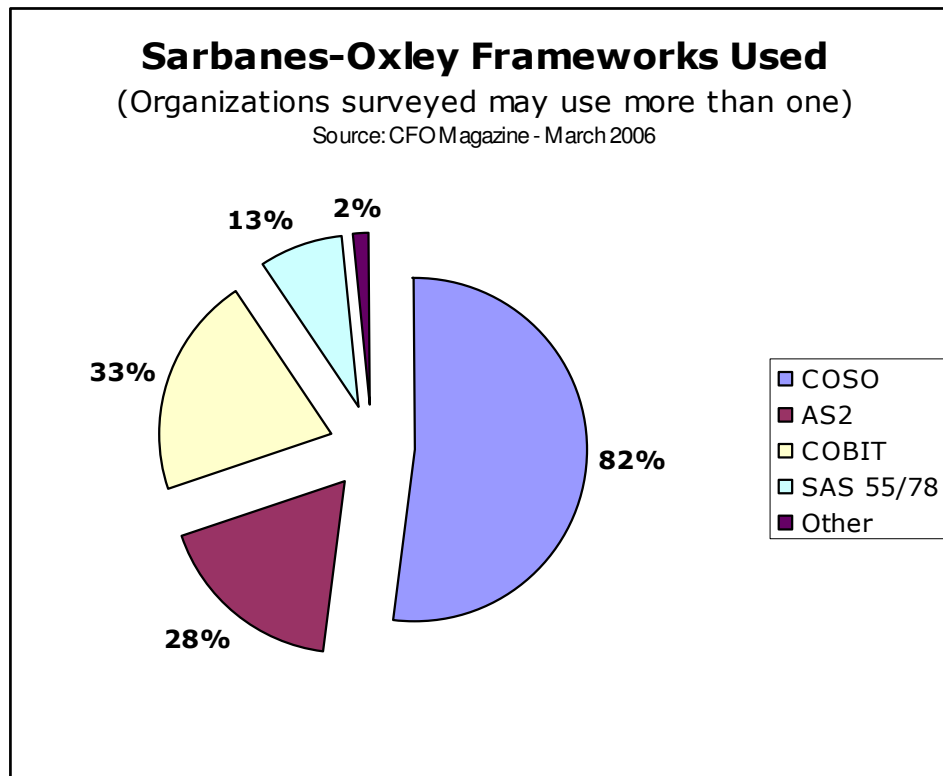
Corporate revenue is reduced by 5% per year due to fraud.

Source: Association of Certified Fraud Examiners - 2005

RELATIONSHIP TO SARBANES-OXLEY

Documentation for Sarbanes-Oxley compliance requires the organization to look at risks, control activities, policies, procedures, etc. across all operations. This investigation becomes an introspective look at how the organization conducts business from the inside-out, the outside-in, and strictly within (such as between departments, divisions, etc.). If executive management promotes, or does little to prevent, fraud in its dealings with employees, customers, and suppliers, there are likely larger problems to first overcome than Sarbanes-Oxley compliance. However, assuming that this is not the case, the examination of how an organization conducts business for the purposes of Sarbanes-Oxley compliance parallels the analysis for supply chain fraud detection and reduction.

In both cases – Sarbanes-Oxley documentation and supply chain fraud detection and reduction – we must identify the monitoring mechanisms (that will be used to detect supply chain fraud), the control activities (that will be used to prevent supply chain fraud), and the policies and procedures (for reducing or addressing existing supply chain fraud).



COSO – SARBOX – SUPPLY CHAIN FRAUD

The Committee Of Sponsoring Organizations (COSO) internal controls framework highlights the following 5 key components which are a useful guide for the detection and reduction of supply chain fraud. In summary:

CONTROL ENVIRONMENT

The “tone” of the organization as set by example and action of senior management. If executives display a cavalier attitude towards ethical practices and professional behavior, even to the point of the commission of fraud, this negative behavior will trickle down to all ranks of employee as being acceptable and could be perpetrated against not only the organization, but also customers and suppliers.

RISK ASSESSMENT

All risks must be assessed for, among other characteristics, their likelihood, damage impact, costs of correction, and costs of prevention. In terms of supply chain fraud, supplier metrics and the vendor scorecard are useful tools in determining suppliers that may be putting the organization “at risk”. Viewing the internal supply chain in a similar way can help identify bottleneck processes, information gaps, software deficiencies, etc.

CONTROL ACTIVITIES

The control activities are the policies, procedures, validations, verifications, etc. that are used to ensure that all levels of business operations function correctly because there is sufficient oversight. Control activity documentation should include not just how, for example, suppliers and employees are supposed to act, but also how they will interact – the organization with its suppliers, customers, and itself (between departments and groups).

INFORMATION & COMMUNICATION

The information an employee needs to perform their job functions efficiently and effectively must be provided based on the employee’s security clearance or level of job function. To withhold such information may force the employee to create unsecured data files that, if stolen or lost, could contain competitively sensitive information about the organization.

MONITORING

The effectiveness of all control activities, such as those used to detect and reduce supply chain fraud – whether manual or systematic – must be constantly evaluated for accuracy and relevance as the organization grows and changes. Like the control activities themselves, the monitoring should not be invasive or excessive as such to inhibit performance or job function.

DEFINITION: SUPPLY CHAIN

I hesitate greatly to offer any definition of the supply chain, as there are likely so many better ones to be found. However, knowing that there are likely a wide variety of definitions available, I do feel somewhat safe in adding a new one to the mix.

The total movement of raw materials, services, finished goods, and monies between suppliers and their customers, from product inception to final product disposition.

Key to this definition and for the purpose of understanding that the supply chain is both internal and external, is that there is something moving between a “supplier” and a “customer”. One party is providing goods to another party.

In the external supply chain, the “customer” is the company who purchases, and the “supplier” is the company who sells to the customer. A company purchasing raw materials takes these goods from a supplier in exchange for (a typically monetary) payment.

In the internal supply chain, the “customer” can be thought of as the department or group receiving something from a “supplying” department or group. A simple example is when the warehouse receives finished goods from manufacturing. However, this could also be true of the relationship between the shipping department and the billing department: when a shipment is sent to a customer, notification must be given to the accounting department to invoice the customer for the goods that were shipped.

Just because something of value (i.e. money) is not the basis for, or exchanged as part of, the transaction, the concept of the supply chain is no less valid. In fact, in this example, the value of the merchandise to the customer represents more than the merchandise on the warehouse shelf, as receivables are assets to a company, and the sale price should be higher than the item cost. Thus, merchandise *value* can be viewed as transferred from the shipping department to accounting department.

The “holistic” view of the supply chain must consider both the internal and the external supply chain. The concept of the supply chain does not stop at the organization’s walls.

The concept of the “supplier” and the “customer” is applicable to both the external *and* internal supply chain.



DEFINITION: FRAUD

There may be fewer definitions of fraud available than those for the supply chain, but much like defining the supply chain, I feel that there are enough in existence such that adding one more for this purpose will not dilute or disrupt the other definitions out there.

A purposeful deception, misrepresentation, or concealment of facts intended to cause injury or loss to another party, typically for the sake of one's own direct or indirect gain.

The employee's gain need not always be direct. An employee who falsifies data in a report to a regulatory agency because the employee is loyal to the organization and wants to protect the employer from possible fines or legal action is still guilty of committing fraud.

Executives, directors, managers, and supervisors cannot simply turn a blind-eye with regards to the actions of those reporting to them – management is responsible for the employees reporting to them and is assumed to have knowledge of their actions.

It is important to emphasize that we are all human and subject to committing errors. It is when the "errors" are done on purpose and with the intent to benefit, either indirectly or directly, that fraud is likely to exist.

Fraud in the supply chain is not necessarily related to "lowest cost". It would be a mistake to assume that fraud exists just because, for example, the purchasing manager opts to conduct business with a supplier whose materials or services are not the cheapest. In fact, good supply chain practices necessitate relationships with reliable suppliers, where the characteristics of a "reliable" supplier should include quality (of materials or services) delivered on time. And it's these solid supplier relationships that can pay for themselves many times over when the customer has an emergency requiring help from their suppliers.

However, all things being equal, the purchasing manager who opts to conduct business with a particular supplier because of gifts, loans, or kickbacks may be guilty of committing fraud. But there may be a fine line between a gift and a loan or kickback, especially if the organization did not outline what is and is not acceptable supplier behavior in regards to gifts and monies to employees. Executive management must set the organization's tone and lead by example, taking care to communicate in writing directives to all those involved.

Fraud is committed with purpose and intent.

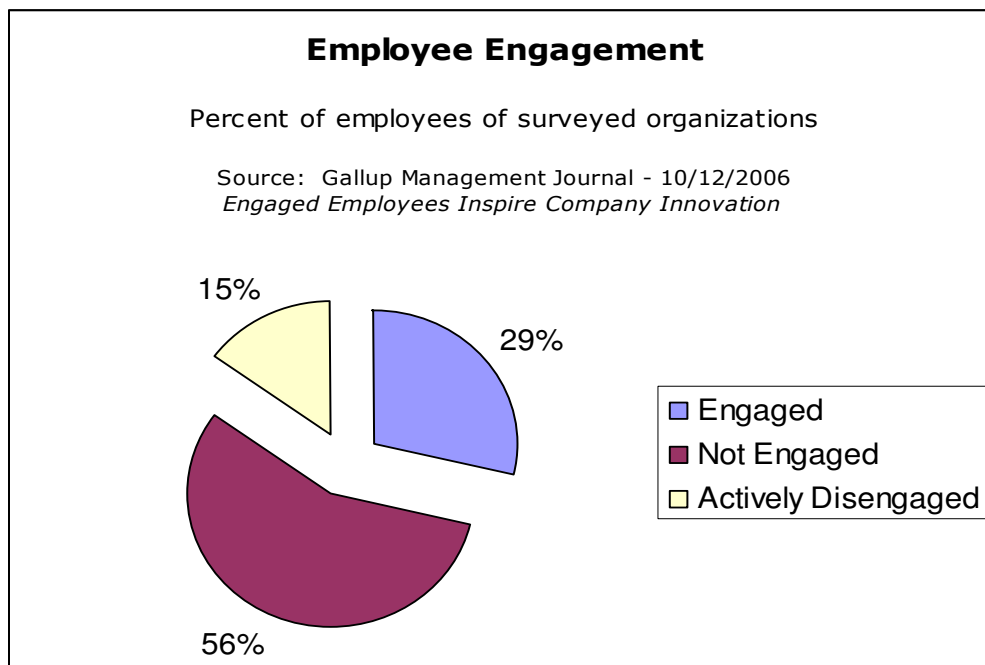
WHO'S INVOLVED?

Fraud, especially those related to the supply chain, will encompass internal, external, and mixed (internal and external) types of collusion scenarios. In brief:

Internal fraud will be perpetrated solely within the organization, without the known involvement of an outside entity, such as a customer or supplier. This may involve an individual or several people on the inside collaborating together to perpetrate the fraud.

External fraud will be perpetrated by an external entity, such as a customer or a supplier, with no knowledgeable or willing person inside the organization as an accomplice.

Mixed frauds will involve collusion between an external entity (i.e. customer, supplier) and one or more internal persons (i.e. full-time employee, contract employee, consultant, etc.).



- **Engaged** employees (**29%**) are innovators and drive organizations forward.
- **Not Engaged** employees (**56%**) “do their time” during the workday, but are also water-cooler chatters and Internet-surfers for a significant amount of the workday.
- **Actively Disengaged** employees (**15%**) are those who purposefully and intentionally thwart and subvert the progressive activities of the organization and other employees.

WHAT CAUSES FRAUD?

There are many theories and psychological studies as to why a person commits fraud. Some of the different theories propose that fraud is committed due to:

- The Western culture that emphasizes material goods in association with social status, where we are forced to “keep up with the Joneses”.
- External pressures beyond our control, such as the healthcare costs of sick parents or children, daycare expenses, etc.
- Pressures we may not be able to control, such as gambling and drug addictions.
- The lack of good morals and values being imprinted upon a person by their social groups, especially beginning at a young age.
- Revenge against the organization due to poor pay, being overlooked for advancement, overworked, etc.

In regards to supply chain frauds, while revenge against the organization is a strong candidate for perpetrating fraud, another culprit is the internal pressures that build within to either increase performance or decrease task times. This is typically the result of management pressures to cut costs without providing the necessary tools to achieve the new performance goals, or due to the establishment of unrealistic benchmarks.

For example, if the manufacturing department is pushed to produce more without any increase in staffing or machinery, at some point supply chain fraud is likely to occur, whether the fraud is the falsification of production output or the production of inferior quality goods. And while the manufacturing department will be held to blame for the failure to produce first-quality goods, it is really the fault of management. The manufacturing employees, out of fear of losing their jobs, may have reverted from “flight or fight” to “fraud or flight”, opting to perpetrate fraud rather than lose their jobs. Fear becomes the motivation to perpetrate fraud, with the sole intent of retaining employment.

Supply Chain ↑ Pressures	Supply Chain ↓ Pressures
<input checked="" type="checkbox"/> New Orders / Recurring Orders	<input checked="" type="checkbox"/> Order Entry Time
<input checked="" type="checkbox"/> Picks Per Hour	<input checked="" type="checkbox"/> Manufacturing Time
<input checked="" type="checkbox"/> Manufacturing Throughput	<input checked="" type="checkbox"/> Picking Time
<input checked="" type="checkbox"/> Receipts Per Hour	<input checked="" type="checkbox"/> Receiving Time
<input checked="" type="checkbox"/> Quality Assurance Testing	<input checked="" type="checkbox"/> Quality Assurance Time

WHERE IT HAPPENS

With an understanding that the supply chain is both internal and external to an organization, supply chain fraud can occur at any link in the chain, for example:

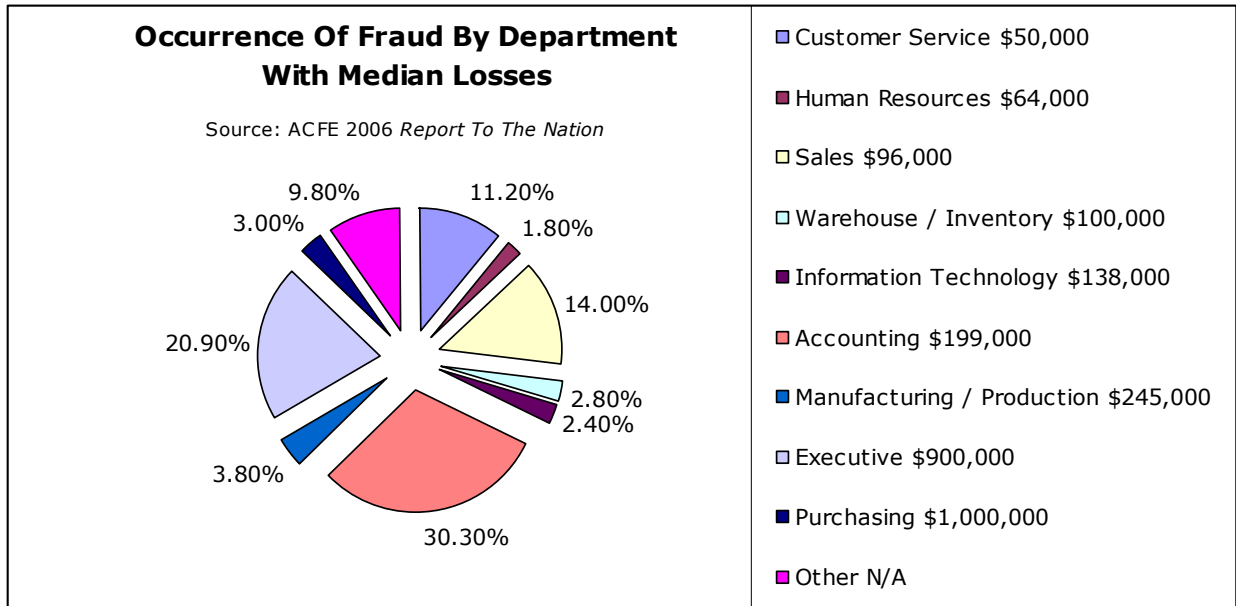
- Fixed Assets**
- Trigger Events**
- Purchase Orders**
- Picking**
- Returns**
- Packing**
- Distribution**
- Shipping**
- Receiving**
- Quality Assurance**
- Inventory**
- Manufacturing**
- Invoicing**
- Sales Commissions**

Common Supply Chain Fraud Categories:

- Asset Misappropriation – Misuse / Abuse**
- Asset Misappropriation – Theft**
- Contract & Procurement**
- Financial**
- Payroll**
- Regulatory – Government & Industry reporting**

SUPPLY CHAIN FRAUDS

With perpetrator possibilities being both inside and outside the organization, where is fraud likely to occur?



Of particular interest:

- The **average** loss across these departments was \$310,222, with an approximate weighted average (excluding Other departments) of \$314,011.
- While **Purchasing** had one of the lowest occurrences of fraud at just 3%, this department also had the highest median loss at \$1M.
- **Accounting** had the highest occurrence of fraud at 30.3%, but it was significantly lower than several other departments, and its median loss of \$199,000 was significantly less than the average median loss.
- **Executive management** was responsible for perpetrating both the second highest occurrence of fraud (20.9%) and the second highest median dollar amount (\$900,000).

IMPACTS OF SUPPLY CHAIN FRAUD

In the short-term, the impacts of supply chain fraud can include reduced cash-on-hand and lower profits. Small-time frauds may turn into big-time crimes. The more fraud is seen as being acceptable, and even profitable, by employees, the more fraud will be committed by more employees who may have been “on the fence” previously about the commission of fraud. And this attitude may spill over to customers and suppliers who become engaged by employees to commit fraud against the organization.

More fraud is discovered by tips from employees, customers, and suppliers than is discovered by audits.

Source: Association of Certified Fraud Examiners

Fraud early in the supply chain can have a ripple effect and eventually lead to serious product liability claims, product recalls, excessive warranty payouts, negative press, and lawsuits when the fraud results in products that are unsafe or fail to live up to their warranted life. The costs of correction after-the-fact are typically much higher than the costs of prevention, yet too few organizations realize the value in this simple equation. Damage-control costs can be considerably higher than the value of fraud detection and reduction programs, especially considering that some damages may not be repairable.

Organizations can be found guilty of criminal misconduct, just like individuals.

Existence of effective compliance programs can *reduce* penalties.

Lack of effective compliance programs can *increase* penalties.

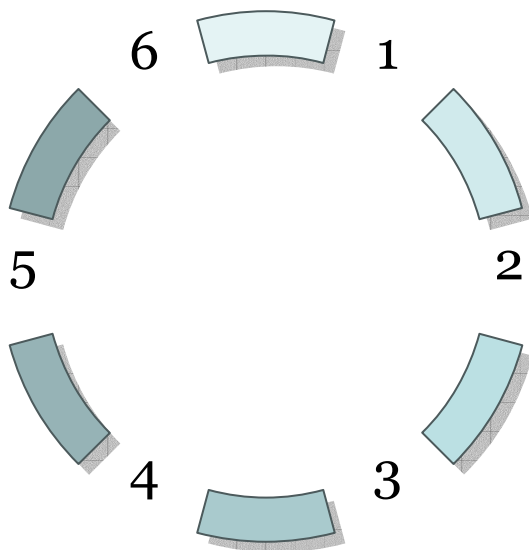
Source: United States Sentencing Commission

SUPPLY CHAIN FRAUD DETECTION

The detection of supply chain fraud encompasses a variety of techniques and methodologies, processes and procedures, and relies on the availability of accurate data in electronic form. It is no longer possible to sift through mountains of paperwork in hopes of manually catching inconsistencies, though this is not to say that a document review would never be in order. Rather, it is necessary to employ analytical programs that can review the increasing volume of information on a timely basis and report anomalies to be reviewed further both programmatically and manually.

To accomplish this requires the movement away from paper-based operations. Readily available and reliable technologies, from barcode applications to Electronic Data Interchange (EDI) are cost-competitive and easily integrated to many Enterprise Resource Planning systems, which are typically the electronic heart-and-soul of an organization's operations.

A primary goal is to close the data gaps – places where paperwork exists and data may not well validated for accuracy and integrity. As the data begins to flow smoothly between these previously manual points, the information can be used to validate other transactions and catch anomalies or fraud.



- 1 = Purchase Order
- 2 = Shipment
- 3 = EDI ASN
- 4 = Receipt
- 5 = Quality Assurance
- 6 = Invoice

SHRINKAGE: BOTTEMLESS PIT OR GRAVE?

Many organizations just write off losses – especially raw materials and finished goods – to **shrinkage**: a general ledger bucket of seemingly endless depth and widespread use for all sorts of ills that may plague an organization. As long as shrinkage is within some acceptable percentage range, no one typically gives it too much thought or care.

If the “acceptable” shrinkage range is arbitrary, i.e. not based on industry standards or market studies, this may be the initial indication of the attempt to cover up fraud.

One problem, therefore, is that all the root causes of the shrinkage are not investigated. Certainly, human error – honest mistakes – will be partially to blame. And while technologies such as barcode scanning and radio frequency identification (RFID), especially when coupled with effective business processes and employee reward programs, can help to reduce the effects of human error, they cannot be expected to fully eradicate error or fraud.

Shrinkage is mostly thought of as due to theft, but the fraud of theft can take many forms and represent different internal and external collusion scenarios between the organization and its customers and suppliers. While no fraud investigation should presume guilt, the root-cause analysis as to the reasons for the inventory shrinkage should include the possibilities of uncovering fraud. As such, having just organization employees conduct such an investigation may be like asking the fox to guard the proverbial hen house.

The affects of inventory shrinkage include:

- ☑ Inaccurate inventory counts
- ☑ Finished Goods not available to fill sales orders
- ☑ Raw Materials not available for manufacturing

ASSESS BEFORE THE AUDIT

Many organizations find themselves at odds with the findings of their auditors about the organization's risk mitigation policies and procedures. The cause of the conflict is likely due to the fact that the auditor requires adherence to standards and guidelines that are not cost-effective for the organization to implement to address some risks. It's not necessarily that the risk does not exist, but the risk must be analyzed on the basis of frequency and impact, not solely on the basis of risk's nature alone. Both parties will agree that the risk exists, but they will differ, often widely, on the likelihood of the risk occurring and the impact of the risk to the organization, and thus the organization's financial commitment to reduce the risk. Bad blood between both parties is a likely result, but it shouldn't have to be this way.

The solution to this "SarBox Struggle" is that the organization should perform a thorough assessment *before* the audit takes place. This is, in fact, one of the requirements of Sarbanes-Oxley compliance as per the COSO framework, if not also others: the continual monitoring and assessment of controls and policies to ensure they are effective and relevant. However, if your organization is not performing regular assessments you're more than likely to be hit with an unacceptable audit review and requirements for the implementation of tough standards and strict policies to address perceived risks.

As part of the assessment by the organization, the justification for the levels of risk management should be documented *before* the audit. The organization must show the balance between the risk (should it occur) and the cost to reduce the risk. The organization has shown its own due diligence in performing the risk assessment, and will likely be in a better position to negotiate what is / is not acceptable risk mitigation with the auditor.



Risk \$ versus Reduction \$

An assessment of risks should be made routinely and *before* the audit, and include:

- Frequency
- Impacts
- Costs
- Damage Control

ARE YOU BUDGETED FOR FRAUD REPERCUSSIONS?

If your organization is not budgeting for fraud detection, prevention, and reduction, then you better be budgeting for fraud repercussions. In much the same way as supply chain fraud cuts across the operations of the enterprise, the repercussions from supply chain fraud are just as far-reaching, (if not actually more so), and much more damaging and costly:

- Manufacturing Downtime**
- Machinery Flush / Clean / Repair**
- Sourcing Replacement Suppliers**
- Customer Credits (Distributor, Wholesaler, Retailer)**
- Consumer Lawsuits (from injury or death)**
- Delayed New Products To Market**
- Delayed Advertising Campaigns**
- Damage-Control Advertising Costs**
- Vendor Compliance Chargebacks**
- Product Recall Costs (shipping, handling, destruction)**
- Loss Of Brand Trust**
- Loss Of Market Share To Competition**
- Regulatory Investigations & Audits (costs & disruptions)**



The ramifications and costs of supply chain fraud can leave your organization left hanging for dear life.

You don't want this to be your neck either.



SUMMARY

Supply chain fraud can encompass the entire breadth and depth of an organization, and its impacts can have a ripple effect throughout both the internal and external supply chain. The techniques, methodologies, and tools to detect and reduce supply chain fraud are available – organizations must realize the value of being proactive versus the costs of reacting to disasters time and time again. Investing in supply chain fraud detection and reduction can help streamline organizational processes and improve efficiencies as a by-product of minimizing risk, and parallel the examination required for Sarbanes-Oxley compliance and documentation.

ABOUT THE AUTHOR

Norman Katz graduated from the University of Florida in 1985 with a Bachelor of Science in Business Administration, majoring in Computer Information Sciences. Norman held positions from Programmer to Business Systems Analyst to Information Technology Manager during his employment career before becoming an entrepreneur. Norman is a Certified Fraud Examiner (CFE) and a licensed Florida Private Investigator.

ABOUT THE COMPANY

Katzscan Inc. (www.katzscan.com) is a consulting firm founded by Norman Katz in January 1996 located near Fort Lauderdale, Florida specializing in: Barcode Applications, Electronic Data Interchange (EDI / eB2B), Data Reporting and Data Conversions, ERP Systems, Software Selection and Implementation, Supply Chain Vendor Compliance (www.vendorcompliance.info), Turnaround Management Help (www.turnaroundhelp.com), and Supply Chain Fraud (www.supplychainfraud.com) detection and reduction.

Sarbanes-Oxley Struggles ⚡ **Supply Chain Fraud Suspicions**
Manufacturing Messes ⚡ **Quality Control Quandaries**
Inventory Inconsistencies ⚡ **Operations Overload**
Chargeback Challenges ⚡ **Distribution Disasters**
Technology Troubles ⚡ **Corporate Chaos**

HELP IS HERE!