Exploring Fraud Theory: An Analysis of Modern Internal Control Structures and Their Efficacy

By Julen Pane

To preface, I want to thank Leonard Vona for this incredible learning experience and opportunity. To call him an excellent teacher and mentor would be a gross understatement of his ability and character. Leonard has served as a carefully guiding hand throughout my development of this paper, asking me tough questions and forcing me to think critically on a subject I initially knew very little about. Fraud is ultimately a complex topic that will take many years, many papers, and many years of driven research to deliver solutions. With this paper, I hope to make you think about how you approach fraud and their relation to internal controls with a theoretical and academic approach. I would also like to thank my coworkers at Fraud Auditing Inc. for teaching the basics of accounting on their own volition, sacrificing their time to help me through this experience. I would also like to show my appreciation for the auditing professionals who have spent years compiling research to be used by other professionals and students. Your work and dedication should not go unnoticed, and throughout my academic career I hope to highlight your work and dedication.

This exploratory paper concentrates on the development of internal controls to prevent internal fraud by employees, management, and associated parties. While external fraud perpetrated by organized crime groups, scammers, and other actors is a deeply important topic in fraud risk assessment, I believe that most controls must be developed through information technology infrastructure rather than auditing.

I'm going to focus on internal fraud, or 'occupational fraud' as this is an area in which traditional internal control structures have fallen short. Also, I'm going to focus on the United States as I have little relevant contextual knowledge about compliance and industries outside of the US.

By using case studies of internal fraud, we will analyze and find shortcomings of traditional internal control structures in an attempt to derive a more comprehensive methodology for the future.

When starting this paper – I was at 0. I had almost no industry knowledge in the auditing sector, so I developed analogies to help understand the concepts laid out by professionals. Here is what I came up with: An organization is like a balloon, air comes in and goes out the main intake/outtake in the form of income and legitimate costs. Every internal party, vendors, employees, and managers are on the inside of the balloon helping things run efficiently. They all have some degree of power to poke holes and divert funds or tear the balloon, which seems impossible to manage. The current anti-fraud structure creates internal controls meant to avoid too much power falling into one party's hands through separation of duties and other general controls. This fails, as internal parties have relative independence on how they use their pin, and the only thing

guiding their usage is the risk to reward of poking a hole for them. So how does an organization do this? Pour water through the balloon and see where there are outflows and vulnerabilities. The only way to find fraud is to analyze data on a massive scale and uncover layers to funds exiting the organization, making it too risky for internal parties to pop the metaphorical balloon. Keep this idea in mind while creating a fraud outline. I will revisit this analogy later in the paper with additional context. For this paper, I will go into why impacting the individual's risk/reward is the best and only method of anti-fraud mitigation.

An Historical Perspective on Fraud Offers Insights

Fraud has existed as long as businesses have operated, with the earliest written example stretching all the way back to 300 BC. As technology has developed and businesses have grown, fraud has advanced with it. Auditing grew as a service during the global colonization process, when the advent of international trade in European nations with the rest of the world resulted in large conglomerates with thousands of workers like the Dutch East India Company. As a network of merchants developed with trading companies, internal auditors were responsible for verifying that all traded goods and valuables were accounted for, but VOC books and financial statements were at risk of being modified by management. Shareholders turned to short selling and shareholder activism to increase internal visibility and protect themselves from fraud. This was one of the first examples of shareholders pushing for ethical management and improved governance within an organization. The idea that shareholders ultimately had power over management was important for instilling in merchant businesses that management

answered to shareholders rather than shareholders being at the mercy of their partners. As time progressed into the industrial revolution, businesses began expanding at rapid rates, with companies issuing shares to the public becoming commonplace, expanding the list of potential stakeholders beyond simple loans and over-the-counter stock trading. Larger companies, more transactions, more employees, and more investors all led to the creation of a stronger corporate governance standard primarily driven by shareholder demands, as would be the case throughout history. In the specific case of occupational fraud, there are few written historical examples of it before the second world war. There is no reason to believe it was less commonplace but was most likely not discovered very often. Organizations had little motivation to uncover threats they were relatively unaware of by hiring external auditors, and especially since computers aids were not invented, auditors would not have been very effective in uncovering fraud risks. Post-war, businesses were growing quickly fueled by a manufacturing and technology boom, and fraud was developing alongside it. Unfortunately, the value of data was not able to be harnessed by technologies of the time, and auditors had far less information available than they do now.

As a form of defense mechanism for businesses unable to control fraud risks in their now massive organizations, auditors turned to developing organizational infrastructure to mitigate these vulnerabilities. Due to information asymmetry and a general lack of widespread adoption of internal controls, the effectiveness of internal controls during the pre-1970s era is difficult to measure, although before RICO adoption, the threat of organized crime fraud risks was far more severe than it is today.

Laws Ushered in Legally Mandated Internal Controls

In 1979, the FCPA or Foreign Corrupt Practices Act was passed into law. This was the first-time the law demanded internal controls to ensure that companies weren't bribing foreign officials to secure business. This was a landmark in the adoption of internal controls nationwide as multinational corporations that were too large to manage on a transactional basis had to be stopped from taking advantage of unstable political environments to secure outsized profits. While this was the first time that internal controls were put into law by the US government, they were primarily referring to internal compliance rather than internal accounting practices. The act required that public companies have a sufficient set of internal accounting controls, but there was no specification on what particular controls were required. The law left it up to each company's auditing/compliance departments to ensure assets were not being misused. To clarify, these controls were for the purpose of ensuring reliable financial reporting for public companies primarily to avoid off-book accounting for paying bribes and maintaining slush funds.[1]

In 1985, COSO(Committee of Sponsoring Organizations) was formed as a result of several cases of fraudulent financial reporting during the previous decades, and the auditing profession was searching for a new method to manage fraudulent financial reporting. They turned the term internal control into a predefined process created and

[1] "A Resource Guide to the U.S. Foreign Corrupt Practices Act Second Edition." n.d. https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl.

followed through by management, building on top of the loosely defined compliance process in the FCPA.

Interestingly, since COSO released its first guidelines for the process of internal control design, it has not changed significantly. It was built around a core 5 concepts: control environment, risk assessment, control activities, information and communication, and monitoring. These components have largely stayed the same over the past 32 years (at the time of writing), and there is no inherent problem with this. Besides the Sarbanes-Oxley Act post-Enron that made new demands for public company accounting including the creation of the PCAOB, the internal control process demanded by law and by auditors has remained largely the same. Specifically, internal fraud has largely been unanswered by law with the DOJ managing situations case by case. Unfortunately, this means that fraud risk detection methodology have remained relatively static.

Internal Controls Continue to be Inadequate, Opening the Way for Fraud

Ultimately, internal controls processes fall short in the risk assessment part of the process since the current fraud risk assessment framework maintains an extremely high-level perspective without factoring in the infinite number of scenarios within a singular fraud risk. While high-profile fraud cases like Boeing, Wells Fargo, and unemployment insurances during the COVID-19 pandemic have all been made public, the ACFE estimates that up to 5% of annual revenue is lost to fraud in some form.

How have auditors been unable to develop internal controls to find these fraud risks? Are they permutations of known fraud risks, or completely unknown risks? Ultimately, the common standard for fraud risks and the previously defined lists of fraud risk are based on past examples of fraud that auditors were able to find, which is a logical fallacy in itself. It is nonsensical to act in a purely reactive measure when most internal perpetrators of fraud have knowledge of the internal controls in place, especially when fraud risk assessments are so high-level that many of them are not specifically tailored to an individual firm's fraud risks. By nature of perpetrators understanding pre-existing internal controls, they are committing fraudulent acts while specifically avoiding the existing controls. Especially since many fraud risk descriptions are far too high level to be used on the small scale that occupational fraud typically exists in, controls act more like a blinder for auditors that can't see what goes on with the multiple permutations that a fraud risk may have.

With this paper, I will go through several real-life cases in which internal controls failed to protect an organization from financial harm, legal damages, and brand damages. I will also look at why vulnerability testing conjoined with regular auditing is one of the most important things an organization can do. Internal controls need to be specifically tailored to fit and protect an organization's most important assets, rather than following basic risk assessment guidelines.

Counterfeit Parts Plague Boeing

A current – as of this paper being written – fraud case that has been in the headlines for a few weeks has been Boeing, a major airplane manufacturer and defense contractor that was found to have used counterfeit materials in constructing planes.

The issue was tied to a lack of oversight of one of the suppliers. This caused significant legal and brand risks to Boeing.

The internal control in place for these airplane manufacturers to protect against counterfeiting fraud was a certificate of authenticity provided by the materials manufacturer.[2] For an airplane manufacturer, the plane construction and the subsequent safety proceedings are the most important part of their brand. However, Boeing's internal control framework lacked sufficient internal controls to ensure that it wouldn't use counterfeit parts.

Vendor product substitution and other kinds of fraud risk are weighted the same by the ACFE Fraud Risk Guidelines. However, using counterfeit parts in an airplane manufacturing are much different in terms of risk to the consumer and brand compared to counterfeit parts in office supplies. While Boeing's fraud risk assessment is not public information, the fact that the only known internal control in place was a certificate of authenticity provided by the manufacturer protecting their most important asset is a

[2] Isidore, Chris. 2024. "Counterfeit Titanium Was Found in Boeing and Airbus Jets. The FAA Is Investigating How It Got There | CNN Business." CNN. June 14, 2024. https://www.cnn.com/2024/06/14/business/faa-probe-counterfeit-titanium-boeing-airbus/index.html.

major fraud oversight. This certificate of authenticity can be explored deeper and shows an underlying problem when assessing fraud risks.

Having the supplier issue a certificate of authenticity places complete trust on the supplier to adhere to all of Boeing's safety specifications although Boeing suffers the brunt of the risk upon fraud coming to light. We can obviously see that Boeing's fraud risk assessment was insufficiently tailored to their own risks.

Besides that, when the perpetrator is aware of the internal control in place and can find a way around it, they have a profit incentive to spend less on parts especially if Boeing is not regularly auditing to ensure legitimacy.

To put it simply, there was an incentive problem between the responsibility and risk for the parts vendor. When assessing its fraud risks, an organization must look at their most important assets and the subsequent legal/brand risks that come with fraud related to them. Especially when these are factors in maintaining the most basic parts of the business, the party at risk must have a majority responsibility in mitigating or supervising those third parties who can place the organization at risk.

Only now will Boeing make an effort to verify all parts coming from suppliers, after losing millions of dollars in legal costs and in future revenue. I don't intend to call out Boeing, but they serve as an example of what happens when quality control is undermined by fraud.

When managing important assets, regular auditing is required and in depth preparation of the various fraud risks that the business may face is the only way to

prevent fraud. Any internal or external party that contributes to the final goods sold by the company must be regularly and thoroughly audited and be aware of the fraud risk assessment that the company has prepared.

By increasing fraud risk preparedness across an organization, all parties that present a fraud risk and wish to maintain a business relationship with the firm will be incentivized not only to self-audit and hold themselves to higher standards, but to hold others accountable. This creates the anti-fraud culture that the ACFE upholds, where internal parties maintain a relative amount of self-regulation since the organization shows a high standard of anti-fraud maintenance.

Wells Fargo Consumer Banking Scandal Reveals Internal Control Deficits

The Wells Fargo fake checking and savings account scandal was a major failure of internal control processes at one of the largest consumer banking companies in the world.

Wells Fargo experienced the growth of consumer banking accounts and unduly placed that pressure on bankers who had a degree of control over account creation. Allegedly, there was company-wide pressure on the bankers to boost the number of accounts, despite having little effect on the number of customers they were able to bring in.[3]

[3] Department of Justice. 2020. “Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts without Customer Authorization.” Www.justice.gov. February 21, 2020. https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices.

In this situation, Wells Fargo failed to adjust their internal control structure in the case of a strategic direction adjustment without realizing that new incentives placed internal employees in a situation that would push them towards breaking compliance structures. Management failed to consider that new strategic directions would open up new opportunities and pressures for employees to commit fraud, and that a company's internal control structure must actively evolve and be considered when implementing new strategic initiatives.

This internal control failure is due to Wells Fargo not adjusting their internal control structure without realizing that a fraud risk assessment and the subsequent controls that must result has to constantly evolve as the organization changes. Fraud changes as business changes, and Wells Fargo failed to adjust its fraud risk assessment as the business and general market changed.

When the core business must make some kind of change, it's important that the fraud risk assessment and internal control structure be updated and considered. The fraud triangle theory applies here. It states that three elements must exist for fraud to occur, rationalization, pressure, and opportunity. When an organization increases one of these three metrics, they must adjust their fraud risk assessment to compensate for it especially given a situation where perpetrators have opportunity. In larger corporations where interaction with upper management is rare, there's an inherent disconnect between employees who are willing to commit fraud and the upper management who are responsible for managing it. The loyalty isn't necessarily to the organization or to

their management, but to keeping their job. Employees who are looking to keep their job especially amid pressure to bring in sales are far more likely to commit fraud especially given that they direct control over sales creation.

The Wells Fargo management failed to look at the underlying fraud risks that result from increased pressure and failed to audit new account creation after the fact, sustaining brand and financial damages to the company. While internal controls can stop some types of fraud, an internal employee is aware of and subsequently can avoid any internal controls process that an organization can reasonably implement. This is why perception of detection is extremely important. The only way to ‘prevent’ fraud by an internal party that would like to preserve their job and avoid legal damages is to make sure that it is widely known that every action where a fraud risk exists is audited and verified by multiple parties.

Increased detection raises the risk significantly for an internal employee, and by raising risk, you eliminate a significant portion of employees whose fraud risk appetite only goes so far. While the maximum realistic consequence an employee can face is termination, the risk comes from how likely termination is to happen when they commit fraud. If every employee believes that they will most likely get fired in the case they commit fraud, you eliminate a portion of those who would commit fraud given the opportunity and pressures, only leaving those who do not care about being terminated. It is ultimately in management’s hands to manage this risk to reward factor in assessing occupational fraud risks.

Lack of Effective Internal Controls Led to Theft at J.P. Morgan Chase

Another example is the case of Kevin Chiu, the wealth manager at J.P. Morgan who stole over $2 million dollars from client accounts to trade in financial markets(for self-gain) or for personal expenses. He would send fraudulent statements to clients saying their funds were still in their accounts when he had drained them in reality.[4]

When senior managers commit fraud, it can be a blindside to the business especially when senior officials are given an extraordinary amount of trust over client's money in the financial services sector. J.P. Morgan chase failed to realize this and develop a simple internal control that could have prevented the situation.

There are fraud risks everywhere within a business, and most risk assessments don't weigh fraud committed by senior managers very high since it is a small and trustworthy group. However, often fraud committed by senior management makes headlines and causes the most significant brand damage. When creating a fraud risk assessment, fraud committed by senior management must be looked at as low likelihood but with awareness that high risk situations can tarnish a firm's reputation across industries. In this case, a simple internal control where an unaffiliated party to the wealth manager would be responsible for delivering financial statements would have

[4]"Former Bank Employee Charged with Million-Dollar Fraud and Embezzlement Scheme." 2023. Www.justice.gov. March 1, 2023. https://www.justice.gov/usao-sdny/pr/former-bank-employee-charged-million-dollar-fraud-and-embezzlement-scheme.

made a difference. It would have been impossible to cover up if funds were lost or drained.

Consider What Risks Could Do the Most Harm

When doing a fraud risk assessment, all parts of the business must be assessed for potential fraud risks even those that seem invincible. It's not about looking at who could act fraudulently, since that could be anyone. Most fraud is committed by people who have done it for the first time. The concentration when looking at a fraud risk assessment is to investigate which parts of the business could cause the organization the most harm if there was fraud. For example, a financial services company suffers the largest legal and financial risks if there is fraud in its money management and trading departments. An oil company would face problems in its refineries if products and employee safety were purposefully not up to safety assurance standards. Food companies would be at risk if distributors chose to sell relabeled and expired products.

While risks like incorrect vendor disbursements are bad for the organization, they cause little to no legal or brand risks. When it comes to tackling small scale shell company fraud, active auditing and increased perception of detection is powerful.

In J.P. Morgan's case, the fraud risk assessment should have taken a close look at how a wealth manager defrauding clients could impact the company and implemented specific procedures for circumventing those risk to the client. Making hypotheticals is extraordinarily important in the case of fraud risk, and foresight is far more impactful than hindsight. The objective is not to investigate and micromanage

employees, but to look at the structural risks that a business has regardless of the employee sitting in a position and to understand and prepare for those specific risks.

How should organizations look at the most important areas of their business and protect them against brand risk? By looking at the permutations that a single fraud risk can have. Theoretically, there are an infinite number of fraud scenarios that exist underneath one fraud risk. Now there is obviously only a certain number of them that are above a negligible percentage chance of realistically happening, but for the core parts of the business and those which could impact the organization legally or culturally, there are dozens of fraud scenarios that management should be prepared to tackle and prevent.

Every fraud risk assessment should have these scenarios and the company should prepare a detection, investigation, and recovery plan for each one. Only by instituting a protective presence over the organization's most important assets can you increase the perception of detection and therefore deter internal parties from committing fraud. There may not be an internal control in place for every single one, as sometimes internal controls slow down companies, but it should be the case that each one of these scenarios is regularly investigated.

To avoid catastrophic consequences in the most important parts of a business, increase the perception of detection by ensuring employees that a fraud risk assessment has been thorough and has uncovered many potential schemes. This is enough to ward off most criminals.

If fraud risk assessments are not looking at the permutations of fraud risks, then internal parties know that the organization will be blind to their actions if they work around the stated internal controls for each risk. Conversely, a competent and thorough fraud detection and compliance component are enough to cut down the number of internal parties willing to perpetrate fraud. Companies must not only be prepared to stop fraud that has occurred but also be ready for what could occur.

Unchecked Power Allowed Fraud at South Florida's University Medical Service Association

Ralph Puglisi was an accounting manager for the University of South Florida's University Medical Service Association, a nonprofit focused on supporting the University's health care wing. He embezzled over $12.8 million dollars from the University as he had unfettered access to credit cards and spending as he was the primary accounting manager. He spent money on personal luxuries, real estate, and allegedly over $6 million on adult websites.[5] This fraud went on for several years, since there was very little spending oversight.

Nonprofit organizations like schools oftentimes lack the necessary resources to detect and manage fraud, often due to thin operational budgets and/or massive varied resources to oversee. Placing unchecked power over funding in one employee's hands

[5] "Former USF Employee Embezzled $12.8 Million, Pleaded Guilty to Mail Fraud." n.d. Baynews9.com. https://baynews9.com/fl/tampa/news/2021/08/13/former-usf-employee-embezzled--12-8-million-and-pleaded-guilty-.

is an unavoidable reality for some small organizations who cannot afford the operational strain of hiring multiple employees to manage their spending and fraud. The best way to manage fraud in this scenario is to hire an external auditor periodically to verify transactions and look for fraud, publicly announcing this audit. This increases perception of detection among internal employees and will turn them away from committing fraud. Prevention is expensive and difficult, but external auditors who are highly tech-enabled can provide increased detection ability across all sorts of organizations. Investing resources into a fraud prevention program is not the best use of time and money for many companies, but looking into fraud detection by consultants or auditors could save time and money.

Internal Controls Prevent Fraud and Protect Assets

The effectiveness of internal controls is not only in the prevention of fraud but also protects asset. In fact, internal controls are effective for protecting a organization's brand more than anything. When dealing with important assets, having an internal control process to ensure that no product is being distributed that may put a consumer at risk is the best use case for controls.

Internal controls work in conjunction with fraud auditing processes, pressuring employees and vendors involved in the final product to adhere to quality assurance procedures. They can serve their purpose when it comes to product regulations and brand risk. For example, internal controls for food companies prevent sale of hazardous products to the public, and internal controls for software companies can prevent data leaks and bad software from being released by a single party. Here, they are useful for

protecting an organization's assets from being manipulated by singular parties, whether on purpose or accidentally.

However, internal controls remain relatively ineffective when an internal party attempts to conceal a threat from the organization. An internal control is good for ensuring that a perpetrator who intends to damage an organization is stopped but remains unable to defend against parasitic entities. Internal controls, by themselves, are not effective in fraud detection or prevention. In some cases, controls can even act as a blinder for auditors when it comes to auditing certain fraud risks, since internal employees understand the control structure and are able to work around it. This was evident with the case of Boeing, where the parts to build airplanes were ensured by a certificate of authenticity, which is a very simple internal control. If there were audits, this aspect was clearly overlooked despite its importance to the organization. Most anti-fraud internal controls can be overridden with corruption, lying, false documentation, and basic manipulation of other internal parties, and currently auditors may see that a control is in place and believe that fraud risks are unlikely underneath it.

Increase Perception of Fraud Detection to Minimize Fraud

Preventing or mitigating fraud is impossible by itself. There is a wide variety of parties with different personal and professional pressures on themselves, and that may outweigh the influence an organization can have on that party. The best an organization can do to minimize fraud is to ensure that the majority, or average low sophistication/low pressure party is less likely to commit fraud. Fraud minimization requires increased perception of detection, which is the concept of internal parties believing that the

organization is regularly being audited and that fraud is likely to be detected. As the ACFE anti-fraud guideline suggests, making a clear anti-fraud statement with assurance that audits are regular and that the organization is prepared to deal with advanced fraud risks is extremely important for an organization. Maintaining an influence on internal parties that they will eventually be caught raises perception of detection, and wards off potential perpetrators by showing that the risk of being caught is not worth the reward. This makes occupational fraud far too risky for an average internal party whose goal is to keep their income and influences internal parties into following the organization's guidelines. The only way to prevent occupational fraud is to ensure that internal parties believe that fraud will be detected, and that they will be unable to simultaneously commit fraud and keep their relationship with the organization.

To explain my point, I'll display a metaphor that I used when I was developing my initial understanding of fraud auditing. This generally applies to monetary fraud risks and helps imagine the misalignment between the effectiveness of internal controls and their purpose. Imagine an organization is like a balloon with the primary air intake being revenue/legitimate costs. Every organization has holes, and this balloon does too. Currently auditors are making sure that people don't poke holes by making sure that everyone on the inside that has a pin follows the rules for using the pin. These rules are a representation for preventative internal controls, as they are generally rendered ineffective by lying, information asymmetry, and corruption especially when fraud risks are not regularly investigated. Of course, some people will lie about how they use their pin since they are independent and for some, the reward of poking a hole is greater

than the risk. They have independence, and the risk/reward is entirely out of the organization's hand since the only factor controlling how people use their pin is their personal risk appetite.

Everyone has a different method, a perpetrator with a pin doesn't stick their pin where the other holes are, rather they poke a new hole that the auditors/investigators don't check for because they don't know it exists. So how should auditors change their approach? Pour water in the balloon and see where it comes out.

Now this may be evidence of my inexperience with auditing, but ultimately the only way to minimize fraud is to change fraud's risk to reward. The consequences of fraud are generally limited, but the odds of being terminated are the only factor the organization can control. By regularly auditing and searching for fraud, you metaphorically pour water through the balloon, and auditors see where the money flows out. This only applies to monetary losses, and in practice is significantly more complex than this. To make this effective, fraud auditors need to be equipped with advanced data analytics tools, statistics, and artificial intelligence tools for processing data.

In practice, this looks like thorough checks of vendors for shell companies, searching for ghost employees, disbursements to dormant vendors, investigations of redemptions, and more. There are theoretically infinite permutations of fraud, and it is impossible for a human auditor to understand patterns in such large amounts of data, which is why I call for usage of AI tools to analyze transaction relationships. Another important factor is separate ledgers for data collection to avoid single party manipulation, which is essentially an iteration of separation of duties. On an

organizational side, committing to higher level data collection will make the audits that much more effective.

An important concept to take away from fraud risk assessments and this paper is that there are a wide variety of parties committing fraud and each one has different risk tolerances. An additional complexity to my previous recommendation is that increased perception of detection applies differently to each party. The average ‘first-time’ fraud committing party risk appetite is only enough if they believe they will not be caught, and therefore an increased perception of detection will make them think that they will potentially lose their job and income, making the risk far outweigh the reward. In the case of a repeat offender or criminal, perception of detection is about how long they can defraud a business before being caught. For this reason, a fraud risk assessment is not one-dimensional, as there are many different interpretations and subsequent consequences. To keep this in mind, auditing has to account for the sophistication of perpetrators where a perpetrator whose goal is to avoid being caught through advanced subterfuge will be significantly more sophisticated than one whose goal is to make some additional money. Understanding why a fraud risk has so many permutations is primarily due to the risk and reward of a crime, and what that means to different kinds of perpetrators. Especially when outsourcing labor, an employer must be careful that they are not inviting perpetrators whose intention is to defraud the organization.

To raise perception of detection across different fraud risks, management must be prepared for the evolution of fraud risks in upcoming years. Looking at where

technology is headed and listening to experts on how to prepare your business for the future is extremely important when assessing fraud risks. These fraud risks are where audits will concentrate, and being able to assess how new permutations will come about in the future will be important for future fraud prevention. Ultimately, showing that management is aware and prepared to detect new kinds of fraud adds a new layer of anti-fraud influence within an organization, and auditors should take responsibility to increase perception of detection when advising organizations on their fraud risk assessments.

Bibliography:

“A Resource Guide to the U.S. Foreign Corrupt Practices Act Second Edition.” n.d. https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl.

ACFE. 2022. “Occupational Fraud 2022: A Report to the Nations.” https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf.

Association of Certified Fraud Examiners. 2024. “Occupational Fraud 2024: A Report to the Nations.” https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf.

“Former USF Employee Embezzled $12.8 Million, Pleaded Guilty to Mail Fraud.” n.d. Baynews9.com. https://baynews9.com/fl/tampa/news/2021/08/13/former-usf-employee-embezzled--12-8-million-and-pleaded-guilty-.

Department of Justice. 2020. “Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts without Customer Authorization.” Www.justice.gov. February 21, 2020.

https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices.

“Former Bank Employee Charged with Million-Dollar Fraud and Embezzlement Scheme.” 2023. Www.justice.gov. March 1, 2023. https://www.justice.gov/usao-sdny/pr/former-bank-employee-charged-million-dollar-fraud-and-embezzlement-scheme.

Isidore, Chris. 2024. “Counterfeit Titanium Was Found in Boeing and Airbus Jets. The FAA Is Investigating How It Got There | CNN Business.” CNN. June 14, 2024. https://www.cnn.com/2024/06/14/business/faa-probe-counterfeit-titanium-boeing-airbus/index.html.

Cotton, David and Leslye, Givarz and Johnigan, Sandra. “Fraud Risk Management Guide: Second Edition.” Association of Certified Fraud Examiners. March, 2024. Fraud Risk Management Guide Second Edition | WebViewer (acfe.com)

PCAOB. 2022. “AS 2401: Consideration of Fraud in a Financial Statement Audit.”

PCAOB. 2022.

https://pcaobus.org/oversight/standards/auditing-standards/details/AS2401.

“Anti-Fraud Playbook - the Best Defense Is a Good Offense.” Grant Thornton. 2020.

https://www.grantthornton.com.vn/contentassets/098617d8536b4df9a94a7dd684b2db85/antifraud-playbook.pdf.