Texas Tech University System
Texas Tech University
Texas Tech University Health Sciences Center

Report on Fraud Risk Assessment

April 23, 2007
Project #2007033

April 23, 2007

Mr. Jim Brunjes
Vice Chancellor and Chief Financial Officer
Texas Tech University System

Dr. Thomas Anderes
Senior Vice President for Administration and Finance
Texas Tech University

Mr. Elmo Cavin
Executive Vice President for Finance and Administration
Texas Tech University Health Sciences Center

Dear Mr. Brunjes, Dr. Anderes, and Mr. Cavin:

We have completed the Fraud Risk Assessment for Texas Tech University System, Texas Tech University, and Texas Tech University Health Sciences Center (referred to collectively in this report as Texas Tech). This engagement is included in our annual plan for the year ending August 31, 2007. The engagement was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing (Standards).

The objectives of this engagement were to gather perceptions of fraud risks at Texas Tech and to promote fraud awareness and prevention across the campuses. Individuals from various offices at Texas Tech participated in facilitated sessions where they were asked their impressions of fraud risk at Texas Tech. These participants perceived conflicts of interest, bribery and incentives, and billing schemes to pose the highest risks in terms of likelihood, pervasiveness, materiality, and reputational risks.

We will consider audits for the 2008 annual audit plan based on the results of this risk assessment. We also plan to develop fraud awareness training that will help equip management at various levels with the skills and resources to prevent and detect fraud. Additionally, we believe the information in this report will be useful to you as you consider how to mitigate overall risks to your respective institutions, including the risk of fraud. While we will continue conversations with you related to fraud considerations, we are not requesting a formal response to this engagement report.

The results of this engagement are provided to assist the management of Texas Tech in enhancing its operations and managing its risks. We appreciate the courtesies and considerations extended to us during our engagement. If you have any questions or if we can be of further assistance, please do not hesitate to contact our office.

Sincerely,

Kimberly F. Turner, CPA
Chief Audit Executive

FRAUD RISK ASSESSMENT RESULTS

OBJECTIVES

While we believe that most employees, students, and other constituents of Texas Tech act ethically and in the best interest of Texas Tech, it would be naïve to believe that fraud does not or will not occur. This engagement is the first in a series of planned work to increase Texas Tech's understanding of fraud.

The objectives of this engagement were to gather perceptions of fraud risks at Texas Tech University System, Texas Tech University, and Texas Tech University Health Sciences Center (referred to collectively in this report as Texas Tech) and to promote fraud awareness and prevention across the campuses.

RISK ASSESSMENT PROCESS

During the planning of this engagement, our office evaluated the potential for different fraud schemes to occur at Texas Tech. We eliminated certain schemes from this risk assessment because of the low probability to occur at Texas Tech. For example, unlike corporate environments, there is little incentive for Texas Tech to misstate its financial statements. In addition, we did not include certain fraud schemes, such as those related to falsifying non-financial information, because we plan to focus on those schemes in future risk assessments.

This engagement involved nine risk assessment sessions where we gathered the perceptions of 52 Texas Tech employees regarding the likelihood, pervasiveness, materiality, and reputational risks of 24 different types of fraud schemes. The fraud schemes considered during this assessment, along with their descriptions, are included on pages 3 through 7 of this report.

During risk assessment sessions, we used electronic polling software that allowed the participants to share their perceptions anonymously. Although this data gathering process was not statistically based, the participants provided our office information that will be valuable in assisting Texas Tech's Board of Regents and management in avoiding or mitigating fraud risks.

RESULTS AND PLANNED ACTIONS

Mitigating Controls for High Risk Areas

Graphs depicting the results of the fraud risk assessment sessions are included in this report on pages 8 through 13. Participants from all three institutions perceived conflict of interest fraud schemes as being highly likely and pervasive across the institutions, as well as having the potential for high materiality and reputational risk. Texas Tech University and Texas Tech University Health Sciences Center participants perceived bribery and incentive fraud schemes as another potential area of high risk. Texas Tech University System participants perceived bribery and incentive schemes as having a high materiality and reputational risk (the highest materiality and reputational risk of all schemes presented) but not as high a likelihood and pervasiveness as the other institutions perceived. Finally, Texas Tech University System participants perceived billing schemes to be high risk (high likelihood, pervasiveness, materiality, and impact to reputation).

Our office plans to incorporate some audit work in our annual audit plan for fiscal year 2008 related to conflicts of interest, bribery and incentives, and billing schemes. The purpose of this work will be to evaluate the controls Texas Tech has established to mitigate fraud risks. Some of these controls will be decentralized at the departmental level while others may be centrally

established. As our annual audit planning process begins, we will consider whether it is appropriate to include audit steps to test mitigating controls in our regularly scheduled audits or if it is more appropriate to include separate engagements for the high risk areas identified during this assessment.

Resources and Skills

Our office plans to take a proactive role in combating fraud at Texas Tech by promoting the awareness of fraud risks. First, we will be developing fraud awareness training. We believe it is especially important to provide training to certain departments in the fiscal affairs divisions, such as the purchasing, payables, and travel offices. These administrative departments process most of the financial transactions for the institutions, and as such, play a critical role in fraud detection and prevention efforts.

We will also offer training to departmental directors and administrators in the various schools and colleges. Management at various levels across Texas Tech has a role in fraud prevention. Chairpersons, directors, managers, and other levels of management are responsible for preventing and detecting fraud. For management to prevent and detect fraud, they must be equipped with the necessary resources and skills. Our office can best help management fulfill this role by educating them on the fraud risks and related mitigating strategies.

In addition, we will dedicate time to be available to assist departments across Texas Tech as they consider fraud mitigation strategies to incorporate into their practices. As a result of the risk assessment sessions, some participants have already contacted our office for more information on fraud schemes so they can further analyze the risks in their areas.

The Role of the Chief Financial Officers and Other Members of Management

A strong ethical foundation is essential in an organization's efforts to prevent and detect fraud. Texas Tech operates in a complex and operationally diverse environment. Thus, efforts to promote and communicate expectations of ethical behavior must be widespread rather than centralized in one or only a few departments. In academic institutions, all members of management are ethics advocates, whether the roles are official or informal. As senior members of management at Texas Tech, we ask that you continue to support fraud prevention and detection efforts by continuing to promote appropriate ethics and values at Texas Tech.

REPORT DISTRIBUTION

Audit Committee, Texas Tech Board of Regents
Mr. Kent Hance
Dr. John E. Opperman
Dr. Jon Whitmore
Dr. Bernhard Mittemeyer

FRAUD SCHEMES

FRAUD SCHEMES CONSIDERED

The following listing discusses the fraud schemes that were considered during the fraud risk assessment sessions. This listing is not all-inclusive and addresses only the fraud schemes considered during this assessment. The information was obtained from the *Fraud Examiners Manual* published by the Association of Certified Fraud Examiners.

CONFLICTS OF INTEREST

Purchase Schemes—Turnaround Sales: A special kind of purchasing scheme sometimes used by fraudsters is called the turnaround sale or the flip. In this type of scheme an employee knows his employer is seeking to purchase a certain asset and takes advantage of the situation by purchasing the asset himself (usually in the name of an accomplice or shell company). The fraudster then turns around and resells the item to his employer at an inflated price.

Sales Schemes—Writing Off Sales: A type of sales scheme involving tampering with the books of the victim company to decrease or write off the amount owed by the company in which the employee has a hidden interest.

BRIBERY AND INCENTIVES

Bid-Rigging Schemes: A vendor offers something of value to the employee to influence the awarding of a contract. The way competitive bidding is rigged depends largely upon the level of influence of the corrupt employee. The more power a person has over the bidding process, the more likely the person can influence the selection of a supplier. Therefore, employees involved in bid-rigging schemes, like those in kickback schemes, tend to have a good measure of influence or access to the competitive bidding process.

> **Need Recognition Schemes:** The typical fraud in the need recognition phase of the contract negotiation is a conspiracy between the buyer and contractor where an employee of the buyer receives something of value and in return recognizes a "need" for a particular product or service. The result of such a scheme is that the victim organization purchases unnecessary goods or services from a supplier at the direction of the corrupt employee.
>
> **Specifications Schemes:** Specifications are prepared to assist vendors in the bidding process, telling them what they are required to do and providing a firm basis for making and accepting bids. One corruption scheme that occurs in this process is the fraudulent tailoring of specifications to a particular vendor.

Kickback Schemes: Kickbacks are the giving or receiving anything of value to influence a business decision without the employer's knowledge and consent. They involve the submission of invoices for goods and services that are either overpriced or completely fictitious. Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and vendors.

Bid Pooling: Bid pooling is a process by which several bidders conspire to split contracts up and assure that each gets a certain amount of work. Instead of submitting confidential bids, the vendors discuss what their bids will be so they can guarantee that each vendor will win a share of the purchasing company's business.

FRAUD SCHEMES (continued)

CASH

Cash Larceny: A cash larceny may be defined as the intentional taking of an employer's cash (the term cash includes both currency and checks). A cash larceny scheme can take place in any circumstance in which an employee has access to cash. Most larceny schemes involve the theft of incoming cash, currency on hand, or theft of cash from the victim organization's bank deposits.

Theft of Cash from the Register (of Cash on Hand): A large percentage of cash larceny schemes occur at the cash register. The most straightforward cash larceny scheme is to simply open the register and remove currency or checks.

Reversing Transactions: Some employees conceal cash larceny by processing reversing transactions, which cause the register tape to reconcile to the amount of cash on hand after the theft. By processing false voids or refunds, an employee can reduce the cash balance reflected on the register tape.

Register Manipulation: Instead of using reversing entries, an employee might manually alter the register tape.

Altering Cash Accounts: Another method for concealing cash larceny is to alter the cash counts on registers. When cash from a register is totaled and prepared for deposit, an employee records the wrong amount so that the cash on hand appears to balance with the total on the register tape.

Cash Larceny from the Deposit: At some point in every revenue-generating business, someone must physically take the company's currency and checks to the bank. This person will have an opportunity to take a portion of the money prior to depositing it into the company's accounts.

Deposit Lapping: Lapping occurs when an employee steals the deposit from day one, then replaces it with day two's deposit. Day two is replaced with day three, and so on. The perpetrator is always at least one day behind.

Deposits in Transit: A strategy used to conceal stolen deposits is to record the missing money as deposits in transit, which is a way of accounting for discrepancies between the company's records and the bank statement.

Skimming: Skimming is the removal of cash from a victim entity prior to its entry in an accounting system. Employees who skim from their companies steal sales or receivables before they are recorded in the company books. Skimming schemes are known as "off-book" frauds, meaning money is stolen before it is recorded in the victim organization's accounts.

Sales Skimming: The most basic skimming scheme occurs when an employee sells goods or services to a customer, collects the customer's payment, but makes no record of the sale. The employee simply pockets the money received from the customer instead of turning it over to his employer.

Receivables Skimming: It is generally more difficult to conceal the skimming of receivables than the skimming of sales because receivables payments are expected. In order to conceal a skimmed receivable, a perpetrator must somehow account for the payment that was due to the company but never received. There are a number of common techniques fraudsters use to conceal the skimming of receivables.

Forcing Account Balances or Destroying Transaction Records: Among the most dangerous receivables skimming schemes are those in which the perpetrator is in charge of collecting and posting payments. If a fraudster has a hand in both ends of the receipting process, he or she can falsify records to conceal the theft of receivables payments.

Lapping: Lapping customer payments is one of the most common methods of concealing receivables skimming. Lapping is the crediting of one account through the abstraction of money from another account. It is the fraudster's version of "robbing Peter to pay Paul."

Writing Off Account Balances: Some employees cover their skimming by posting entries to contra revenue accounts such as "discounts and allowances." If, for instance, an employee intercepts a $1,000 payment, he would create a $1,000 "discount" on the account to compensate for the missing money. Another account that might be used in this type of concealment is the bad debt expense account.

INVENTORY AND OTHER ASSETS

Inventory and Other Assets: Employees target inventory, equipment, supplies, and other non-cash assets for theft in a number of ways. These schemes can range from stealing a box of pens to the theft of millions of dollars worth of company equipment. The terms inventory and other assets are meant to encompass the misappropriation schemes involving any assets held by a company other than cash. There are basically two ways a person can misappropriate a company asset: the asset can be misused or it can be stolen.

Misuse of Inventory and Other Assets: Assets that are misused but not stolen typically include company vehicles, company supplies, computers, and other office equipment.

Larceny—Purchasing and Receiving Schemes: Dishonest employees can manipulate the purchasing and receiving functions of a company to facilitate the theft of inventory and other assets. Assets are intentionally purchased by the company and later misappropriated by the perpetrator. The company loses both the value of the merchandise and the use of the merchandise.

Larceny—Asset Requisitions and Transfers: Asset requisitions and other documents that allow non-cash assets to be moved from one location in a company to another can be used to facilitate the theft of those assets. Employees use internal transfer paperwork to gain access to merchandise which they otherwise might not be able to handle without raising suspicion. These documents do not account for missing merchandise the way false sales do, but they allow a person to move the assets from one location to another.

FRAUDULENT DISBURSEMENTS

Billing Schemes: Billing schemes offer the prospect of large rewards. Since the majority of most businesses' disbursements are made in the purchasing cycle, larger thefts can be hidden through false-billing schemes than through other kinds of fraudulent disbursements. There are three principal types of billing schemes: false invoicing via shell companies, false invoicing via non-accomplice vendors, and personal purchases made with company funds.

FRAUD SCHEMES (continued)

Invoicing Via Shell Companies/Forming a Shell Company: Shell companies are fictitious entities created for the purpose of committing fraud. They may be nothing more than a fabricated name and a post office box that an employee uses to collect disbursements from false billings.

Invoicing Via Non-accomplice Vendors/Pay-and-Return Schemes: Instead of using shell companies in their billing schemes, some employees generate fraudulent disbursements by using the invoices of legitimate, third-party vendors who are not a part of the fraud scheme. In pay-and-return schemes, employees intentionally mishandle payments which are owed to legitimate vendors. Examples of this scheme include purposely double-paying an invoice and pocketing the second payment or intentionally purchasing excess merchandise, returning the excess and pocketing the refund.

Personal Purchases with Company Funds: Instead of undertaking billing schemes to generate cash, many fraudsters simply purchase personal items with their company's money. The company ends up unknowingly buying goods or services for a dishonest employee.

Payroll Schemes: In payroll schemes, the perpetrator typically falsifies a timecard or alters information in the payroll records. Payroll frauds involve disbursements to employees rather than to external parties. The most common payroll frauds are ghost employee schemes and falsified hours and salary schemes.

Ghost Employees: The term ghost employee refers to someone on the payroll who does not actually work for the victim company. Through the falsification of personnel or payroll records a fraudster causes paychecks to be generated to a non-employee.

Falsified Hours and Salary: The most common method of misappropriating payroll funds is by falsifying the number of hours worked or changing the wage rate.

Expense Reimbursement Schemes: Employees can manipulate an organization's expense reimbursement procedures to generate fraudulent disbursements.

Mischaracterized Expense Reimbursements: Most companies only reimburse certain expenses of their employees. Which expenses a company will pay for depends to an extent upon policy, but in general, business-related travel, lodging, and meals are reimbursed. One of the most basic expense reimbursement schemes is perpetrated by simply requesting reimbursement for a personal expense by claiming that the expense is business related.

Fictitious Expense Reimbursements: Employees sometimes seek reimbursement for wholly fictitious expenses. Instead of overstating a real business expense or seeking reimbursement for a personal expense, an employee just invents an expense and requests that it be reimbursed.

Overstated Expense Reimbursements: Instead of seeking reimbursement for personal expenses, some employees overstate the cost of actual business expenses. This scheme can be accomplished in a number of ways.

Altered Receipts: The most fundamental example of an overstated expense reimbursement scheme occurs when an employee doctors a receipt or other supporting documentation to reflect a higher cost than what he actually paid.

Overpurchasing: Another way to overstate a reimbursement form is the "overpurchasing" of business expenses. This method is typically used by employees seeking reimbursement for travel expenses. The employee makes two purchases, one for a lower purchase price and one that is more expensive. The employee utilizes the less expensive purchase but attaches the receipt of the more expensive purchase for reimbursement. The more expensive purchase is returned to the vendor for a full refund.

Multiple Reimbursements: This type of fraud involves the submission of a single expense several times.

Check Tampering: Check tampering is unique among the fraudulent disbursement schemes because it is the one group in which the perpetrator physically prepares the fraudulent check. In these schemes the perpetrator takes physical control of a check and makes it payable to himself through one of several methods.

Forged Maker Schemes: The person who signs a check is known as the "maker" of the check. A forged maker scheme may be defined as a check tampering scheme in which an employee misappropriates a check and fraudulently affixes the signature of an authorized maker thereon.

Forged Endorsement Schemes: Forged endorsements are those check tampering schemes in which an employee intercepts a company check intended to pay a third-party and converts the check by endorsing it in the third-party's name. In some cases the employee also signs his own name as a second endorser.

Altered Payee Schemes: This scheme is a form of check tampering in which an employee intercepts a company check intended for a third party and alters the payee designation so that the check can be converted by the employee or an accomplice. The employee inserts his own name, the name of an accomplice, or the name of a fictitious entity on the payee line of the check.

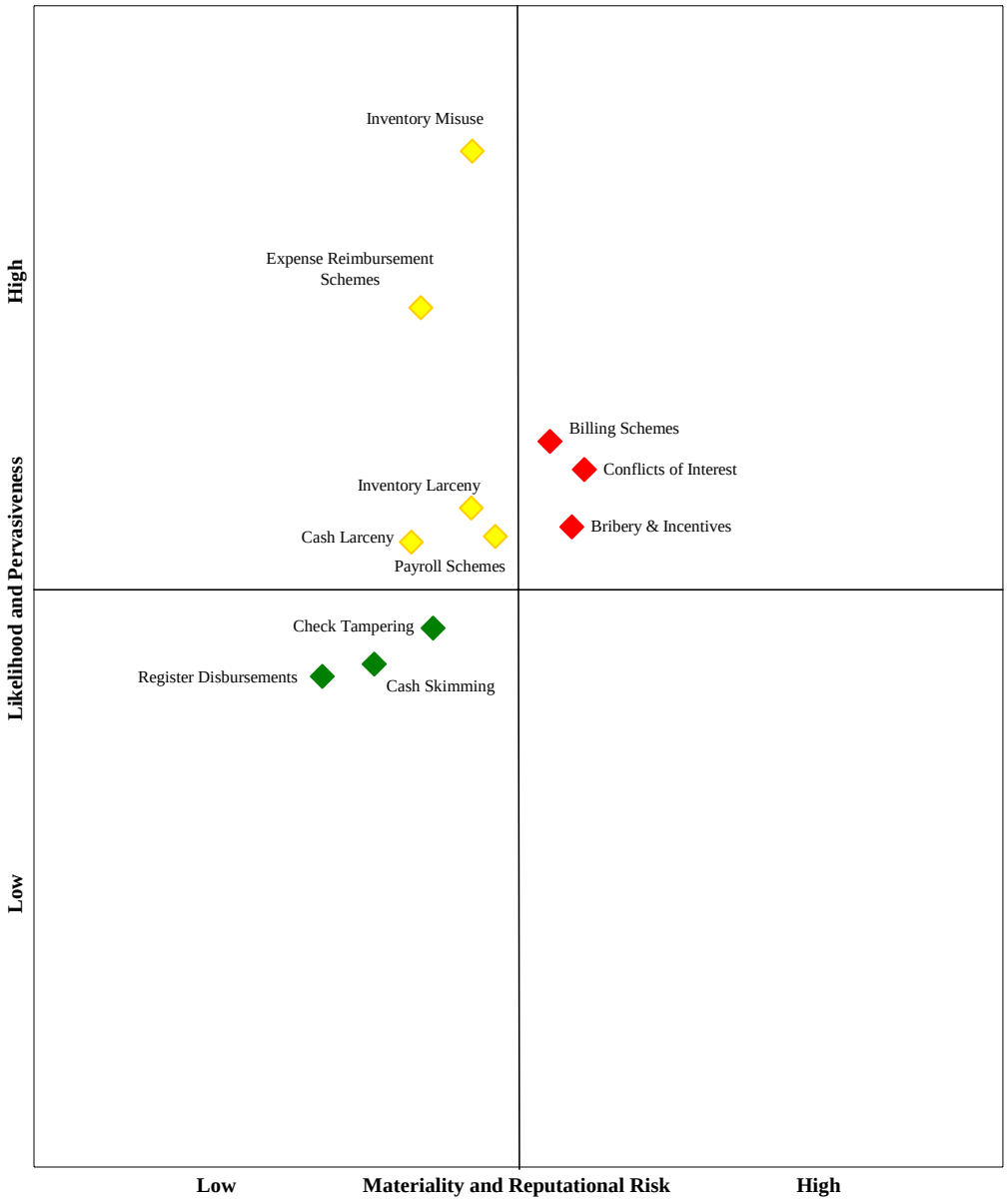
Register Disbursement Schemes: Fraudulent disbursements at the cash register are different from the other schemes that often take place at the register, such as skimming and cash larceny. When cash is stolen as part of a register disbursement scheme, the removal of the cash is recorded on the register tape. A false transaction is entered so it appears that the disbursement of money was legitimate.

False Refunds: A refund is processed at the register when a customer returns an item of merchandise that was purchased from the store. The transaction that is entered on the register indicates the merchandise is being replaced in the store's inventory and the purchase price is being returned to the customer. In other words, a refund shows cash being disbursed from the register to the customer.

False Voids: Fictitious voids are similar to refund schemes in that they make fraudulent disbursements from the register appear to be legitimate. Typically, when an employee sets about processing a fictitious void, he simply withholds the customer's receipt at the time of the sale. In many cases customers do not notice that they are not given a receipt. With the customer's copy of the receipt in hand, the culprit rings a voided sale.

FRAUD RISK HEAT MAPS—TTUSA

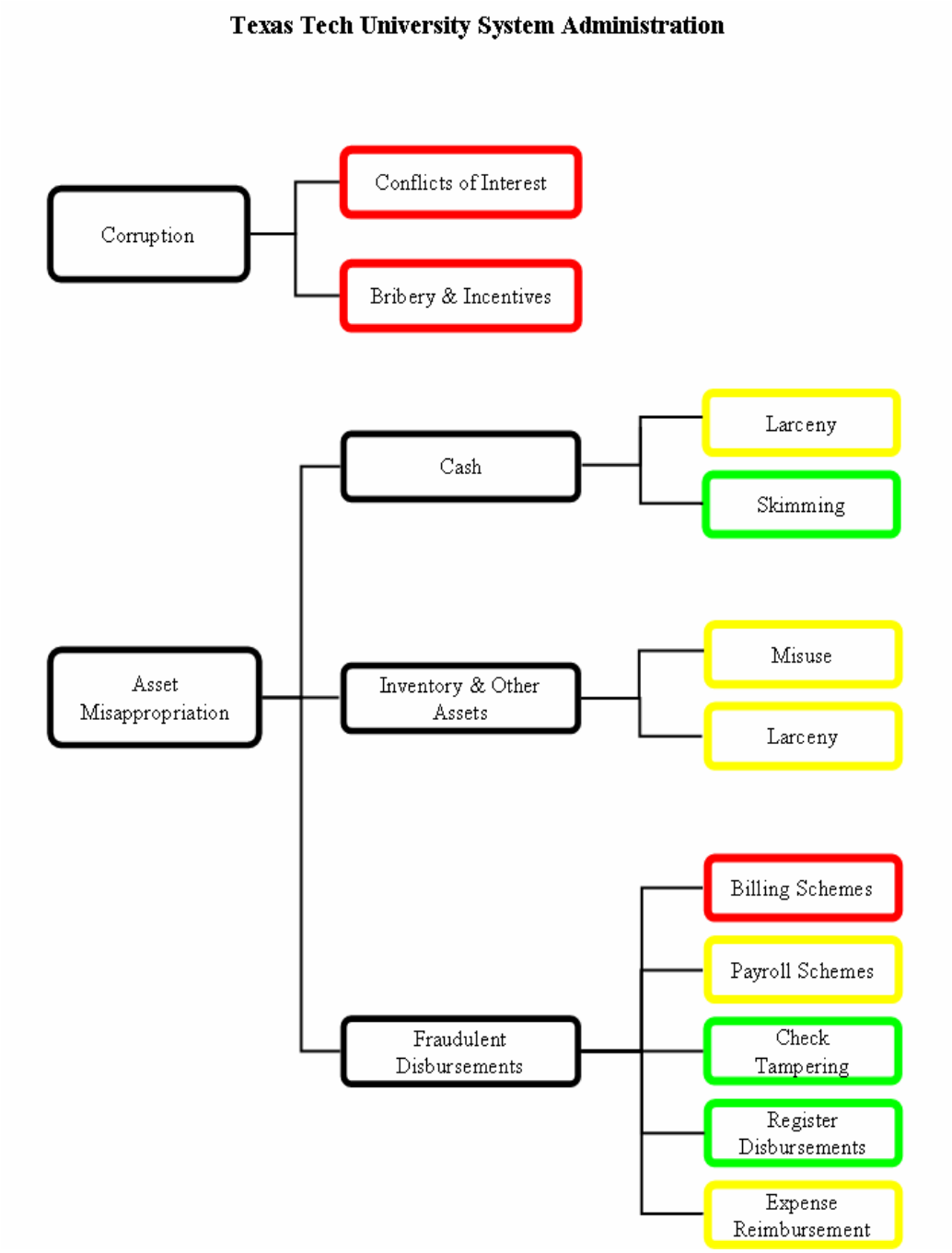
Texas Tech University System Administration



This graph depicts the perceptions of the Texas Tech University System Administration employees who provided input for the fraud risk assessment.

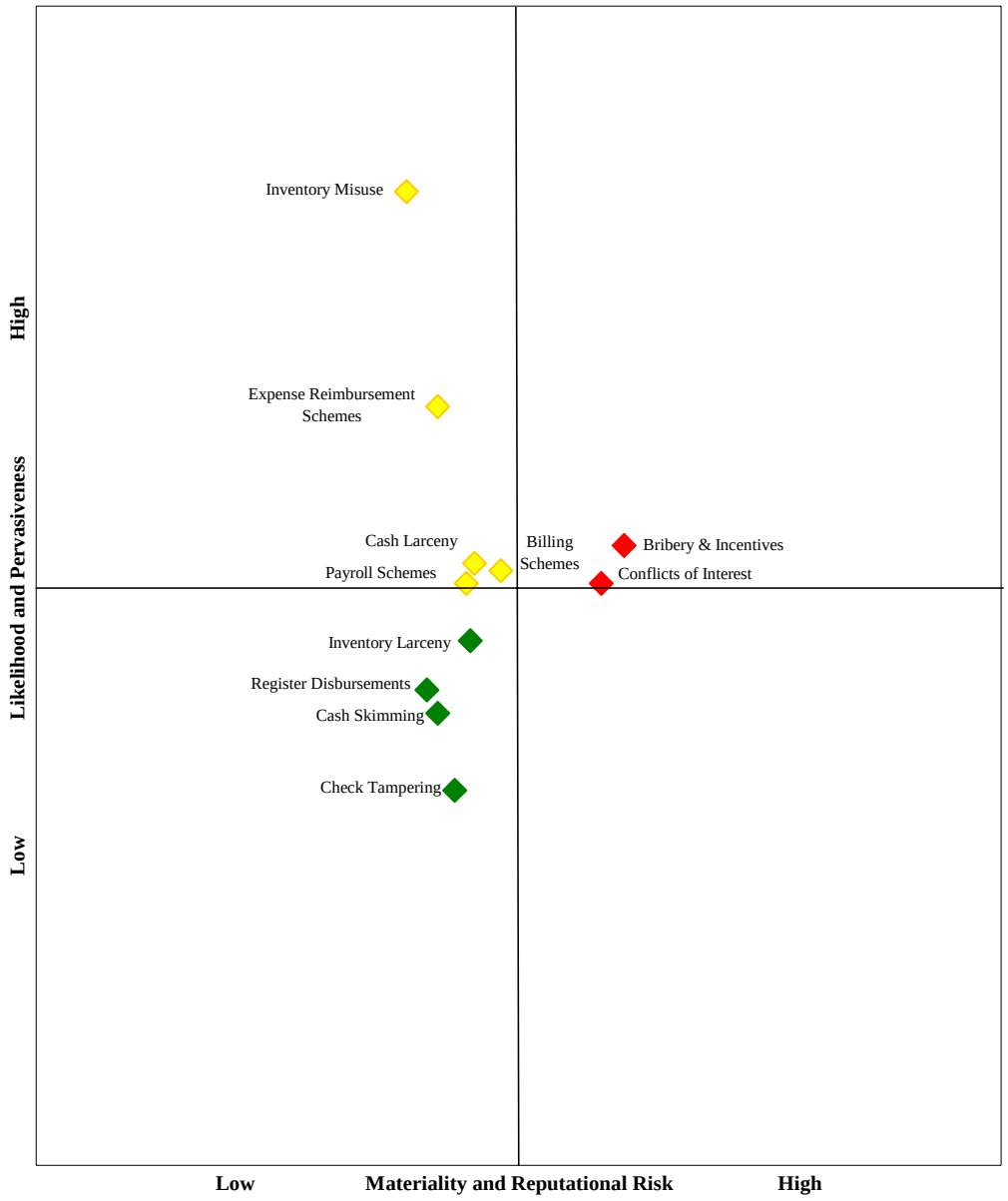
- Perceived to have high likelihood and probability as well as high materiality and reputational risk
- Perceived to have high likelihood and probability, but a low materiality and reputational risk
- Perceived to have a low likelihood and probability and a low materiality and reputational risk

FRAUD RISK HEAT MAPS—TTUSA (continued)



FRAUD RISK HEAT MAPS—TTU

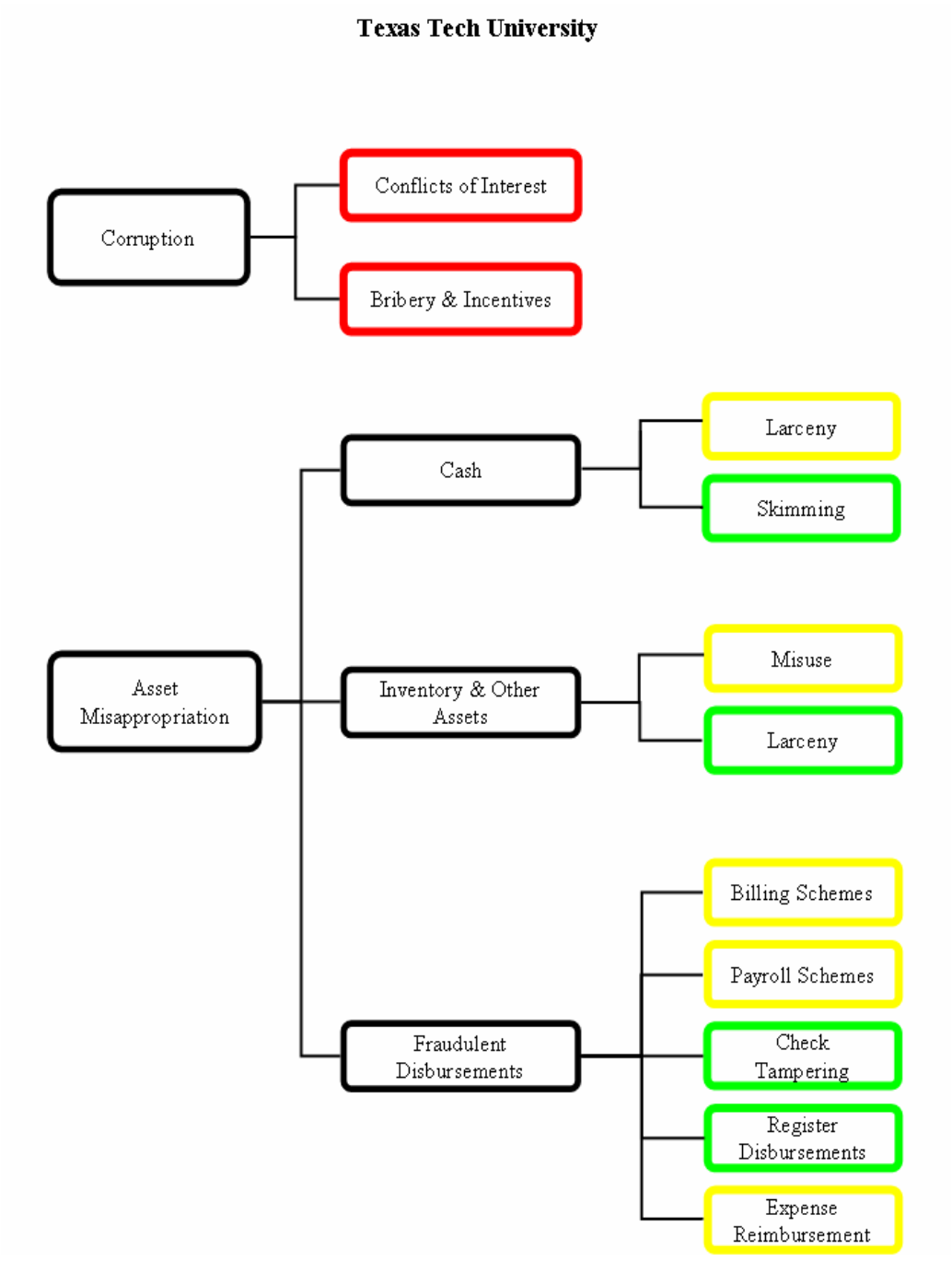
Texas Tech University



This graph depicts the perceptions of the Texas Tech University employees who provided input for the fraud risk assessment.

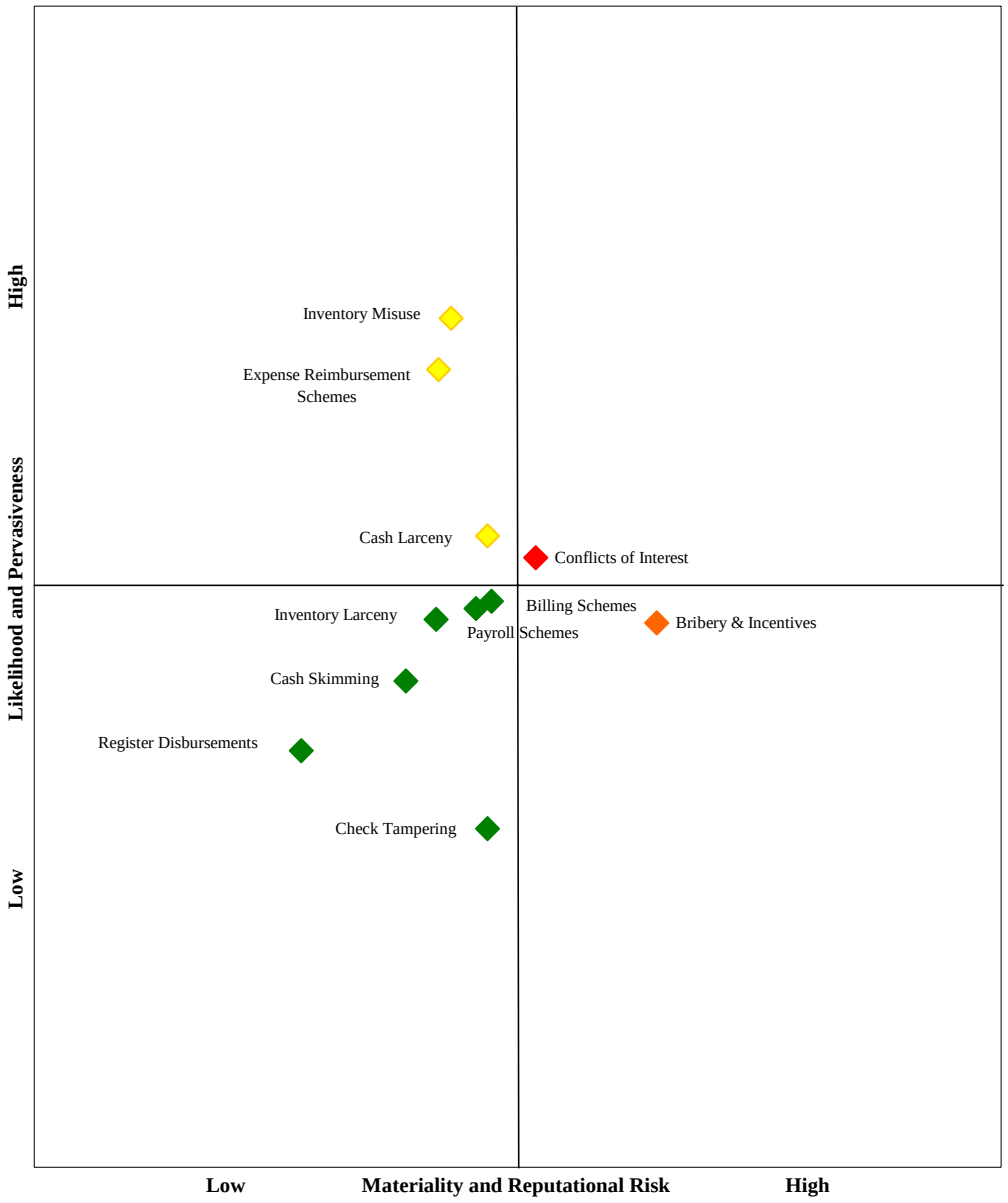
- Perceived to have high likelihood and probability as well as high materiality and reputational risk
- Perceived to have high likelihood and probability, but a low materiality and reputational risk
- Perceived to have a low likelihood and probability and a low materiality and reputational risk

FRAUD RISK HEAT MAPS—TTU (continued)



FRAUD RISK HEAT MAPS—TTUHSC

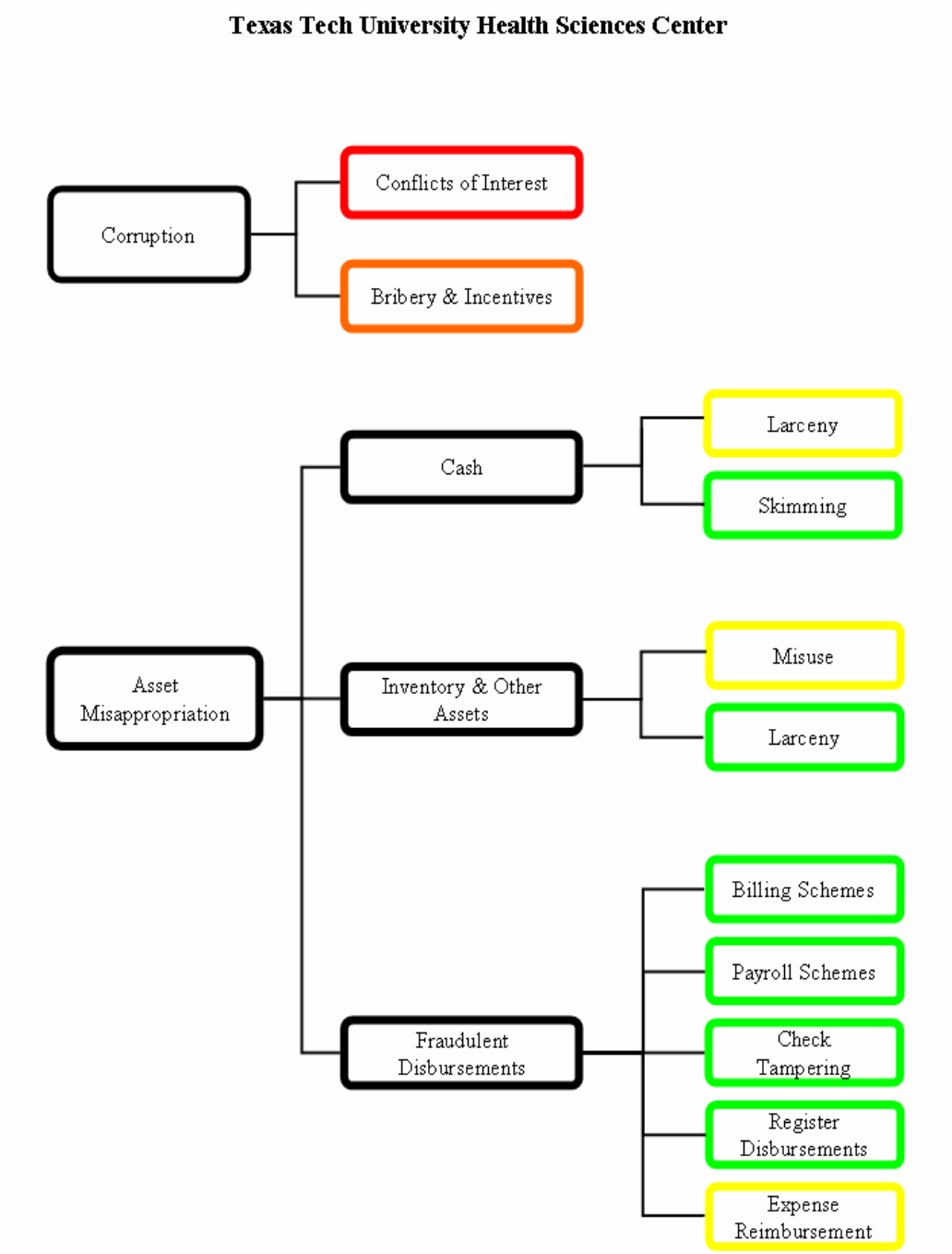
Texas Tech University Health Sciences Center



This graph depicts the perceptions of the Texas Tech University Health Sciences Center employees who provided input for the fraud risk assessment.

- Perceived to have high likelihood and probability as well as high materiality and reputational risk
- Perceived to have high likelihood and probability, but a low materiality and reputational risk
- Perceived to have a low likelihood and probability, but a high materiality and reputational risk
- Perceived to have a low likelihood and probability and a low materiality and reputational risk

FRAUD RISK HEAT MAPS—TTUHSC (continued)



BASIS OF TESTING

SCOPE

We performed this audit in accordance with the International Standards for the Professional Practice of Internal Auditing (Standards). Our audit scope was based on Standard 2110.A2, which states that internal audit should evaluate risk exposures relating to the organization's governance, operations, and information systems.

RESOURCES

Association of Certified Fraud Examiners. (2006). Report to the Nation on Occupational Fraud & Abuse. Austin, TX: Association of Certified Fraud Examiners.

Wells, J. T., (2004). *Corporate Fraud Handbook: Prevention and Detection.* Hoboken, NJ: John Wiley & Sons, Inc.

Wells, J. T., Bishop, T. J. F., Bradford, N. S., Geis, G., Gill, J. D., Kramer, W. M., et al. (2006). *Fraud Examiners Manual*. Austin, TX: Association of Certified Fraud Examiners.