**Chapter 1:**

1. **What are the three basic steps to the fraud process?**
	1. Fraudulent act (dishonest)
	2. Convert (cash)
	3. Conceal (most difficult)
2. **What are the three broad types of activities from the Report to the Nation on Occupational Fraud and Abuse) that are used to define occupational fraud and abuse (OFA)?**
	1. Asset misappropriation
	2. Fraudulent financials
	3. Deliberate misuse
3. **What are some characteristics of OFA?**
	1. Clandestine Hidden/Secret
	2. Violates employees (fiduciary duties)
	3. Committed for direct or indirect benefit of employee
	4. Cost of the business (money or assets)
4. **How does the costs incurred from Fraud and abuse in an organization differ from other "normal" costs (e.g., wages, taxes, rent...\_)?**
	1. Fraud is material
5. **Define "abuse" and list some examples? Do you agree with the text's list of items that constitute abuse?**
	1. Abuse: to take advantage: examples include
6. **What are the legal criteria that must be met to prove fraud has occurred?**
	1. Common law:
		1. Material false statement
		2. Know statement is false
		3. Reliance on statement by the victim
		4. Damages must exist that result from reliance
7. **What is the difference between criminal and civil fraud?**
	1. Civil: evidence weighs heavily
	2. Criminal: innocent beyond all reasonable doubt
8. **Define larceny, embezzlement, conversion.**
	1. Larceny: the taking or carrying away of money or property of another without consent of the owner with the intent to deprive the owner of its use
	2. Embezzlement: willing to take or convert to ones own use someone else’s property
	3. Conversion: The exchange of a convertible type of asset into another type of asset, usually at a predetermined price, on or before a predetermined date.
9. **What does it mean to breach one's fiduciary duty?**

A fiduciary duty is an obligation to act in the best interest of another party. For instance, a corporation's board member has a fiduciary duty to the shareholders, a trustee has a fiduciary duty to the trust's beneficiaries, and an attorney has a fiduciary duty to a client.

1. **How do organizations often treat fraud and abuse differently when punishment is needed?**
2. **Edwin H. Sutherland**
	1. Noted for explaining why people are dishonest
	2. “White collar crime”
	3. Theory of differential association
		1. Theory that crime is learned, not genetic, learned from interpersonal groups (peers)
3. **Donald R. Cressey**
	1. 3 reasons fraud is committed:
		1. Opportunity, Motivation – feel like we can take something without being caught
		2. Pressure- unsharable constraint
		3. Rationalization- reasoning
4. **Richard C. Hollinger**
	1. Most theft from job dissatisfaction, regardless of age or position
	2. Employee perception on controls
5. **What types of people commit fraud**?
6. **What motivates people to commit fraud?**
Greed, Motivation, Opportunity, Pressure, Rationalization, Revenge, Anger

**Chapter 2:**

1. **Define and be prepared to discuss Asset Misappropriations.**

In [law](/topic/law%22%20%5Ct%20%22_top), **misappropriation** is the intentional, illegal use of the [property](/topic/property%22%20%5Ct%20%22_top) or funds of another person for one's own use or other unauthorized purpose, particularly by a public official, a [trustee](/topic/trustee%22%20%5Ct%20%22_top) of a [trust](/topic/trust-law%22%20%5Ct%20%22_top), an executor or administrator of a dead person's [estate](/topic/estate%22%20%5Ct%20%22_top) or by any person with a responsibility to care for and protect another's assets (a [fiduciary](/topic/fiduciary%22%20%5Ct%20%22_top) duty). It is a [felony](/topic/felony%22%20%5Ct%20%22_top), a crime punishable by a prison sentence.

Over the years, the asset misappropriation chart has become known as the “fraud tree” for its numerous branches. The tree’s trunk consists of two major asset types: cash, and inventory and all other assets. Crooked employees clearly favor misappropriating the former—nearly nine in 10 illegal schemes in the study involved the cash account.
The reasons should not be surprising: Cash is fungible, has a specific value and is easily transported. Inventory—except for consumer goods—has limited usefulness to a thief; an employee in a ball bearing plant can have a hard time converting the loot into cash. And of course, many business enterprises don’t have a physical inventory at all.

**SEE FRAUD TREE BELOW (LAST PAGE)\*\***

1. **What is the effect of asset misappropriation on the financial statements?**
* Understated earnings
* Overstated inventory
* Overstated Expenses/Write-off’s
1. **If you were planning review procedures to detect asset misappropriation, just from using the financial statements, how would you proceed?**
* If sales were up 10%, most other accounts should be up by 10%. The familiar financial ratios should all correspond as well.
* Look for strange changes in:
	+ Customer credits or write-offs
	+ Adjustment accounts
	+ Inventory scrap, spoilage, obsolescence
	+ Inventory shrinkage
	+ Fixed asset write-offs
1. **What are the options to conceal asset misappropriations?  How would you plan procedures to detect these?**

**Concealing Asset Misappropriations**

* False debits
	+ To expenses (most common)
		- Expenses are not tangible (can’t be inventoried)
		- Expense accounts closed to zero at end of year
	+ To assets
		- Commonly debit accounts receivable
		- Debit to asset easier to detect
		- Stays on books
* Omitted credits
	+ Concealment technique for cash skimming
	+ Pocket cash, no credit to sales
* Out-of-balance conditions
	+ Asset removed from business (debit)
	+ No corresponding credit
	+ Perpetrator hopes nobody notices
* Forced balances
	+ Variation of out-of-balance technique
	+ Instead of a false entry to cover loss, perpetrator simply adds wrong, carry false totals
	+ Used by perpetrators with access to the books

**Techniques to Prevent Asset Misappropriation**

* Employee monitoring
* Segregation of duties
* Examination of documentation
* Examination of canceled checks
* Independent verification
* Surprise audits
* Job rotation
* Vendor rotation
* Physical security

|  |
| --- |
| http://media.journalofaccountancy.com/JOA/Issues/2001/12/tree.jpg |

**Chapter 3:**

**1) Be prepared to discuss what skimming is and how fraudsters can perpetrate this crime.
      -How does sales skimming schemes leave a victim's books in balance, despite the theft of funds?
      -How does this alter the ability to detect the fraudulent activity?**

-Skimming is the theft of cash from a victim organization BEFORE the cash hits the accounting system.  In a sales skimming scheme, the fraudster collects the customer’s payment at the point of sale, but simply pockets the money without recording the sale or the payment.
(a). Since the money is taken before the transaction is recorded, the accounts don't change.  Because the accounts have not changed, they remain in balance.
(b). If the money is taken before a sale can be recorded, it can be difficult to detect the fraudulent activity.  This will leave no starting point for an investigation and by the time the missing inventory is noticed, it could be too difficult to trace.

**2) How do “understated sales” schemes differ from “unrecorded sales?”**

Unrecorded sales scheme

 In this scheme the fraudster never actually records the sale but collects the payment. The perpetrator may alter or not print the register tape in order to make sure the sale is not recorded.

Understated Sales Scheme

In these skimming schemes the customer receives a receipt that is for the total amount of the transaction but when the employee enters it into the system they record either a discount or a sale of lesser value.

**3) To conceal skimming on the cash register, a fraudster may:**

 -Not print transaction on register tape

 -Ring in transaction as a “No Sale”

 -Use discounts or write-offs

 -Alter the register tape

-Use Lapping (Take customer A’s money and then use customer B’s payment toward customer A’s accounts)

-Void the sale after payment

**4) Things to investigate**

–Conduct surprise cash counts. Reconcile versus sales

 -Look for increasing cost of goods sold and decreasing sales

 -Increase in A/R and decrease of cash

 -Unexplained entries to inventory accounts

**5) Off site sales**

-The salesperson conducts the sale outside the normal business premises. Off site sales are generally less supervised than on site sales, due to their nature, and receipts are more vulnerable. The sales person may issue false receipts and other documents and may direct payments to another address or bank account

**6) What is receivable skimming? Why is this more rarely used?**

 - employee steals the customer’s payment of their receivable account and doesn’t post the payment on the books (Check fraud 🡪 Difficult to conceal)

- EX)- employee takes check, keeps it, and doesn’t post the balance for the checks

 - Problem: check is made out to the company

 - employee takes check to the bank to cash

 - could set up a fictitious company and set up a bank account to cash the check

a) **Why is receivable skimming more rarely used?**

- If a payment on an account receivable is stolen, the receivable becomes past due and collection efforts will be made by the victim company. Of course, the customer has already paid his bill. The only reason the payment has not been recorded is because an employee of the victim organization has stolen the payment. If questioned about the missing payment, the customer will presumably be able to produce a cancelled check verifying that payment was made.

**7) What other skimming techniques are there?**

* + Changing deposits to actually make an account reconcile
	+ Mailroom theft
		- If you have a small business, use a lockbox
		- Checks that are coming back b/c they were sent to wrong address. No one really knows they were supposed to get the money, so people in the mailroom will start to figure it out.
		- “What are all these checks that have come back?”
			* Maybe people that have just overpaid their accounts or something. Mostly small checks.
			* EX) Insurance company making payments on disputed claims—checks came back—gave checks to sister who ran meth lab

**8) What are the most common ways to conceal skimming?**

 - destroy or alter records

- lapping

- forging book balances

- stealing customer’s statements

- inventory padding

- fictitious accounts

**9) List false entries a fraudster can make to conceal receivables skimming. Are any "better" than the others to avoid detection?**

 **-** Accounts Receivable (DR) 1000

Bad Debt Exp (CR) 1000

**10) How can businesses prevent and detect skimming?**

**-** Revenue will be lower than it should be but the cost of producing that revenue will remain constant.

**-** be alert to the following indicators:

 **-** increasing cost of sales

- excessive or increasing inventory shrinkage

 - ratio of cash sales to credit card sales decreasing

 **-** ratio of cash sales to total sales decreasing

 - ratio of gross sales to net sales increasing

 **-** discrepancies between customer receipt and company receipt

 - customer complaints and inquiries

 - forged, missing or altered refund documents

-Controls to set in place to prevent skimming:

 - separate the accounting functions from cash handling;

- hire an independent contractor on an annual basis to take a complete inventory. -- have a CPA review the company’s bank statements on a regular basis.

 - Controls to set in place to prevent receivables skimming:

- segregate the duties of receiving and recording customer payments, posting cash receipts, and preparing the bank deposit.

- all incoming mail should be opened by an employee who is separate from all of these functions

**11) In the case of** [**Stefan Winker**](http://www.allbusiness.com/professional-scientific/accounting-tax-preparation/4012358-1.html)**, what clues were there to indicate his fraud?**

 **-** had control over all the money that came in and out of the company at every stage (either from cash or checks from customers brought in by the delivery drivers; OR by credit customers who sent their checks in by mail)

- no established internal controls over the handling of checks that came in by mail, in effect giving Winkler total authority to manipulate the accounts

 - accounting director had too much freedom

- took cash receipts journals, copies of customer checks, deposit slips, and other financial records, and removed his personnel file. He also altered electronic files, backdating accounts receivable lines to make them current and recording large customer discounts.

 - checks on a route deposit slip with no matching entries in A/R

 - deposit slip in Winkler’s handwriting

 - when Winkler came to Mogel’s, he was had financial problems:

 - he had lost his house and his finances were in disarray

**Chapter 4:**

**1) Define Cash Larceny**

 - Larceny is the least common of the three major cash misappropriation categories.

 - Intentional taking 🡪 Of employer’s cash 🡪 Without employer’s consent

 - “Cash” includes currency and checks

 - Cash Larceny schemes involve the theft on money that has already appeared on a company’s books

**2) What is the difference between cash larceny and skimming?**

 **-** Skimming is theft of *off*-book funds

 - Cash Larceny is theft of *on*-book funds

 - Cash Larceny:

 -Less common than skimming

 -Less costly than skimming

 -Direct audit trail

**2a) Which is more difficult to detect and why?**

 -Skimming 🡪 because the fraud is performed before the transaction is recorded

**3) Where can cash larceny occur according to the text?**

 -Cash and checks recorded on account, Cash registers, Deposits

 **-**Target an organization’s incoming receipts

 -More common in small businesses and especially the *healthcare industry* and *education organizations.*

-Makes up 16% of the health care industry cases but only 10% in general.

 -Accounting personnel were also more likely than other employees to engage

 in cash larceny, payroll fraud, and billing schemes.

**4) How to conceal?**

 -Sometimes they have no plan

 -Treat it as a loan that they will eventually repay

 -“I’m entitled”

 -Take money from another register

 -Death by a thousand cuts

 -$1-2 per day. testing the system

-Write a personal check to balance the register, but just make sure it never gets deposited

 -Alter the cash counts or register tapes

 -Say there’s more money there than there is

 -False voids returns

**5) What are ways to detect larceny?**

* Compare cash register tape totals with cash/checks actually in drawers
* Track voids and returns
* Two people verify the deposit
* Reconcile the bank statement
* FROM BOOK: Analyze relationships between sales, returns allowances, COGS

**6) What steps might an organization take to protect outgoing bank deposits from cash larceny schemes?**

* Keep deposit secure until it is ready to be taken to the bank
* Use pre-numbered deposit slips and sealable deposit bags
* Segregation of Duties:
	+ Custody – cash receipt, cash counts and bank deposits
	+ Record Keeping – deposit receipt recon, bank receipt recon, posting deposits
	+ Authorization – cash disbursements

**7) What are the main weaknesses in an internal control system that permit fraudsters the opportunity to commit cash larceny schemes?**

* Lack of segregation of duties
* Lack of timely bank reconciliation
* Not securing the deposit before it is taken to the bank
* Lack Surprise cash counts
* Lack mandatory vacations and job rotations

**8) In the case study "The Ol' Fake Surprise Audit Gets 'Em Every Time", (**[**starts on page 113**](http://books.google.com/books?id=uF4M9ZydAzIC&pg=PA113&lpg=PA113&dq=The+Ol%27+Fake+Surprise+Audit+Gets+%27Em+Every+Time&source=bl&ots=WLKr1byg8a&sig=wDYyy--B9x6_qKjNkm150v7U6Tk&hl=en&ei=Hru0S4jJO4myNoahvKAJ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CAYQ6)**) how did Newfund's accounting and management controls contribute to the detection of Gurado's fraud scheme?  Will this be effective in deterring future similar frauds?**

They had strong controls in place that included surprise audits conducted by their internal audit group with help from an external group. The audits involved taking complete control: sealing the file cabinets, taking immediate control of the cash drawers and the ledger. They would also do an immediate and complete audit of the branch if anything was suspected and would take immediate disciplinary action.

Yes, everyone in the company knows about the audits, their thoroughness and that action will be taken.

**Chapter 5:**

**1) Assume there are two thefts of checks at ABC company.  In the first case, an employee steals an outgoing check that is drawn on ABC's account, and is payable to D. Smith.  The perpetrator forges the endorsement of D. Smith and chases the check.  In the second case, an employee steals an incoming check from D. Smith that is payable to ABC company.  The employee fraudulently endorses the check and cashes it.  Which of these schemes would be classified as check tampering?**

-The First because check tampering involves fraudulent *disbursement*

**2) What is check tampering?**

-A form of fraudulent disbursement in which a person prepares a fraudulent check for own benefit or converts a check intended for someone else.

**3) What privileges must an employee have to expose an organization to check tampering?**

-May have access to blank checks, work related duties that involve handling signed checks, perpetrator has check signing authority, or if employee controls reconciliation of bank statement. These duties must be divided among employees.

**4) What are some red flags that check tampering might be occurring?**

-Excessive number of voided checks, Missing checks, Non-payroll checks payable to employees, Altered or dual endorsements on returned checks, Alterations to payee, amount on returned checks, Questionable payees or payee addresses, Duplicate or out-of-sequence check numbers

**5) What are the five principal methods used to commit check tampering?**

-Forged Maker Schemes, Forged Endorsement Schemes, Altered Payee, Concealed Check, Authorized Maker

**How is each of the five frauds perpetrated?**

*-Forged Maker Schemes*: access to unsecure blank checks, forge name of authorized signers, usually done by the person who does bank reconciliations, voided checks are not destroyed

*-Forged Endorsement Schemes*: Intercept check intended for 3rd party( usually accomplished by perp having duty of handling and mailing signed checks or signed checks being returned to the company if wrong address is used), forge endorsement, have ally cash check at a bank, credit union, or convenience store.

*-Altered Payee*: Intercept check for 3rd party and change the payee to own name, prepares check in erasable ink prior to giving to authorized signer, or add on to the name of the payee. Example: Check to U.K. becomes check to U. K. Smith

*-Concealed Check*: Prepare check made to self and put in stack of checks hoping authorized signer doesn’t notice or pay close attention when endorsing checks

*-Authorized Maker*: Authorized signer makes fraudulent disbursements. Where controls prevent signer from handling blank checks or bank reconciliations, perpetrator uses influence to override controls.

**How is check tampering concealed?**

-If perp. reconciles the bank statement, he/she marks fraudulent check “void,” destroys bogus checks when statement arrives, incorrectly add totals to make reconciliations match on purpose. If payee/amount was altered, perp. re-alters cancelled checks to match postings. Enter false information into disbursement journal, code checks to very active or dormant accounts, if check to legitimate payee was intercepted then the check may be re-issued so that the payee doesn’t complain, or create bogus support for checks.

**What controls can reduce fraud risk and/or increase detection?**

-Separate duties of: check cutting and posting, check signing, check delivery, and bank statement reconciliation, require proper support for all checks, mail checks immediately after signing, keep A/P records secure, rotate duties.

**6) How do fraudsters gain access to check stock (blank unused company checks)?**

-Checks are not kept in a secure place. Perpetrator has duty of preparing checks.

**7) In "**[**A Wolf in Sheep's Clothing**](http://books.google.com/books?id=uF4M9ZydAzIC&pg=PA119&lpg=PA119&dq=a+wolf+in+sheep's+clothing+fraud+melissa+robinson&source=bl&ots=WLKr1dth27&sig=0GXyeU2EAzhEupzwTVSg04G21E0&hl=en&ei=3PW0S8uSBcKAlAe49O03&sa=X&oi=book_result&ct=result&resnum=1&ved=0CAkQ6)**" Melissa Robinson was able to steal over $60,000 from her employer without being detected.  Why?  What controls were missing or not used?**

-Her employer saw her as a long-time employee and placed too much trust in her, believing that she could never possibly commit fraud against the company. There were supposed to be two authorized signers to each check, but Melissa would often just forge the second name as she was the other authorized signer. The board of directors also never conducted the yearly audit that was supposed to be a requirement, and therefore never checked the financial statements or books, which were handled solely by Melissa, allowing her to manipulate the checks in any manner.

**8) In "What are Friends For?' (class handout) Ernie Philips stole $109,000 via check tampering.  How was this scheme accomplished and what could management have done differently to prevent the fraud from occurring?**

\*\*No Handout Given

**9 EDI or electronic payment may reduce the risk of check tampering.  Do you agree?  Why, or why not?  What are the additional risks created by electronic transactions?**

-Agree. Electronic payment would reduce access to routing and account numbers and therefore the opportunity for counterfeiting. Risks involve computer hackers gaining access to customer credit card numbers and making fraudulent purchases and also employees of businesses from sharing customer credit card information.

**Chapter 6:**

**1) What are register disbursement schemes? How do they differ from skimming and larceny, that also often require taking money from a register?**

-A form of fraudulent disbursement that involves stealing cash from the register. A reversing transaction is made to justify the disbursement and keep the register balanced. Skimming involves taking only a portion of the sales or stealing a portion of the sales before it is on the books. Larceny involves simply stealing money from the register without making an adjusting entry.

**2) What are the two basic fraudulent disbursement schemes?**

-False Refunds and False Voids.

**3) What is the difference between a fictitious refund scheme and an overstated refund scheme?**

-Fictitious Refunds: No goods are actually returned resulting in an overstatement of the inventory.

-Overstated Refund: A legitimate return is made, but perpetrator overstates amount return and skims the excess.

**4) How are fraudulent void schemes used to generate a disbursement from a cash register?**

-The perpetrator makes a sale to the customer and keeps the customer’s receipt. After the customer has left, the perp. uses the receipt to process a false void. If a manager’s approval is needed, the signature may be forged or a signature stamp may be used. The perpetrator then pockets the voided amount.

1. **How are these frauds concealed?  What accounts are affected?**
2. **What control processes make this scheme more difficult?**
3. **In the case study involving Bob Walker (handout during class), what type of register disbursement scheme did he commit.  How does the fraud triangle help to explain his actions?**
4. **Be prepared to discuss the article "Control Cash-Register Thievery."  What was the fraud, how was it detected?**

**Chapter 7:**

1. **What types of billing schemes are discussed in the following articles?**

 *-Shell Companies*: Def- A shell company is a company that exists but does not actually do any business or have any assets.

1. **How are shell companies formed and how are they used to defraud an organization?  What type of "sale" is most often "made?"**-Shell companies are formed by simply going to the local county courthouse and filing paperwork to establish a “DBA”. With this DBA you can open a bank account in the businesses name. Shell company schemesuse a fake entity established by a dishonest employee to bill a company for goods or services it does not receive. The employee converts the payment to his or her own benefit. The most common type of sale is a fraudulent invoice with a description similar to that found on many other invoices, and is below a materiality threshold.
2. **How can the fraudster get fraudulent invoices approved?  How does the ability to collude with another employee or outside vendor help?**- Normally the fraudster will choose a value that is below the company’s, which they are defrauding, materiality threshold or a threshold that requires addition verification to be paid. The fraudster then includes their fraudulent invoice along with a stack of legitimate invoices in the hopes that it will just be approved for payment. Collusion allows people who work in different areas to work together to overcome controls in place to maintain proper separation of duties.
3. **What are some red flags (signs that something is "not right") in relation to shell company schemes?**- Invoices for unspecified consulting or other poorly defined services, Unfamiliar vendors, Vendors that have only a post-office-box address, Vendors with company names consisting only of initials, Rapidly increasing purchases from one vendor, Vendor billings more than once a month, Vendor addresses that match employee addresses, Large billings broken into multiple smaller invoices, each of which is for an amount that will not attract attention, Internal control deficiencies such as allowing a person who processes payments to approve new vendors.
4. **How were Stanley and Phoebe finally detected?  What does this tell you about the process to detect fraud?**- Over a five year period there was a small uptick in consulting fees which led to a vendor review. Next the auditor noticed that Phoebe had put SJR on the books as a vendor nearly 24 months earlier. Since that time, its billings had increased in both frequency and amount. Then the auditor correctly reasoned that consultants generally don’t bill more than once a month, nor do they normally quadruple their billings in one year’s time. He also noted that some SJR invoices weren’t folded and wondered whether that meant they hadn’t even been mailed. Furthermore, SJR Enterprises wasn’t in the phone book. Finally the CPA compared vendor addresses with employees’ home addresses and found that SJR Enterprises had the same address as Phoebe. To confirm his findings the CPA went to the courthouse and obtained a copy of Stanley’s assumed-name certificate; since it was public record. Doing this confirmed that Stanley and SJR Enterprises were one and the same. This fraud would have never been uncovered if Stanley’s wife didn’t come to the Auditor and provide him with a tip that she thought her husband was doing something wrong.
* **Using the information provided from "Billing Schemes, Part 2: Pass-Throughs" be prepared to discuss the following:**
1. **What is a pass-through scheme and how does it differ from a Shell company scheme?  What are the advantages/disadvantages of their use for fraudsters?**- Using a fake company as a 3rd party to pass-thru purchases
2. **What aroused Ben and Julia's suspicions?  What type of audit test indicated that inventory was probably understated?**- Why Lincoln didn’t know how the price went up but knew it would go down
- Year end inventory & Analytics
3. **Detail the controls that make shell company and pass-through schemes harder to implement?**- S.O.D., Up-to-date vendor lists, the purchasers cannot approve vendors, run a credit report on a new company
* **Using the information provided from "Billing Schemes, Part 3: Pay-and-Return Invoicing" be prepared to discuss the following:**
1. **How can an employee generate fraudulent activity using a non-accomplice vendor?**- Use a pay & return scheme (overpay someone & then keep the return)
2. **What was Jenny's scheme and what controls were put in place to deter future thefts?**- Stealing checks & processing some invoices twice
- Train the accounting department to look for this & add an automated procedure to the invoice payment system, reassign responsibilities, & set up an employee hotline
3. **Locate a "Hot Line" service that is online and be prepared to discuss during class.**
* **Using the information provided from "Billing Schemes, Part 4: Personal Purchases" be prepared to discuss the following:**
1. **Be prepared to discuss the threat from personal purchases with company resources and countermeasures to discourage.** - Buying things for ourselves with company money

 - fraudulently authorizing invoices by an appropriate party

 - falsifying documents to obtain authorization

 - altering legitimate PO’s

 - misusing company credit cards

**12b**. - Ensure company policy clearly prohibits all personal purchases with company funds

 - Do not permit the same employee to originate purchases and approve them

 - Separate the invoice approval function from the payment and receiving function.

 -Establish maximum purchasing limits for each employee.

 - Install controls to detect multiple purchases just below employees’ approval limits.

- Establish procedures to routinely check for deliveries of company-ordered goods to external addresses. And look for matches between invoice delivery addresses and employees’ home addresses.

- Examine shipment-receiving reports for merchandise ordered and paid for but not delivered.

- Check invoices for vendors that are not usually associated with the company’s business. For example, it would be suspicious for a manufacturer to order goods from a department store.

- Routinely examine individual employees’ buying habits, looking for increases in the amount or frequency of purchases.

- Carefully control access to, and purchases that are made from, company credit cards. Be especially alert to purchases in round amounts, which might indicate false or inappropriate charges.

1. **What is a good question to ask former employers, know that most will not give a "bad" reference for fear of litigation?**- “Would you rehire this person?”
2. **What are some additional "red flags" in the billing and disbursement area, not discussed previously, that should arouse suspicion that fraudulent activity might be occurring?**- Employee relationships in the workplace

**Chapter 8:**

**1) What are the three main categories of payroll fraud?**

 -Ghost Employees, Falsifying Hours, Commission Scheme

**2) What is a ghost employee?**

 **-**Refers to someone on the payroll who doesn’t actually work for the victim company. The ghost frequently is a recently departed employee, a made-up person or a friend or relative of the fraudster, who can cash the paycheck by forging the endorsement or by having an accomplice deposit the proceeds into his or her bank account.

**3) Within a given organization, who is the individual most likely to add ghost employees to the payroll system?**

 -Payroll Chief or whomever handles the payroll

**4) Through what process is the ghost employee actually paid?**

-Fictitious employees are issued paychecks that are actually deposited in various personal accounts. The controller of the payroll accounts fulfills process.

**5) Be prepared to discuss the others ways that payroll frauds are perpetrated, falsified hours and salary and commission schemes.**

 -Overstatement of employee hours, falsifying overtime hours

**6) What controls and/or tests would prevent and/or uncover payroll fraud schemes? Think about computer aided tests that might be particularly effective here.**

 -Forced vacations, segregation of duties, running comparative checks on addresses, SSN, bank account numbers

**7) In the case of Jerry Harkanell, what internal controls would have prevented the falsification of his timesheet? (Case is in Wells text).**

 **-**

**8) Explain what constitutes expense reimbursement fraud and be prepared to discuss four categories discussed in the text and how these are perpetrated.**

-Mischaracterize expenses

 -Overstate Expenses

 -Fictitious Expenses

 -Multiple Reimbursements

**-What are some controls that would be used to mitigate these types of fraud?**

 -Training 🡪 makes sure you’re paying for valid expenses for valid purposes

**9) Provide one or two examples of how an employee can commit the fictitious reimbursement fraud?**

 -Falsifying write-offs

**Chapter 9:**

**Why is inventory such a popular item to use in fraudulent activity, especially financial statement fraud?**

It is very easy to hide inventory. There are many ways to conceal the fraud. Perpetrators can move inventory around between locations in order to cover up the fraud, they can also just adjust the financial statements to make them balance.

1. **Be prepared to discuss the following four categories of non-cash misappropriation**

 -Larceny: the wrongful taking and carrying away of the personal goods of another from his or her possession with intent to convert them to the taker's own use, perps are usually highly trusted and have access to secure inventory

-Asset requisitions and transfers: divert materials from a job site, very comment in construction industry, classify inventory as damaged or scrap.

-Purchasing and receiving schemes: perp usually involved with receiving/warehousing function, steal portion of incoming shipment (mark as short, reject portion as “substandard”)

-False shipments: perp usually involved in sales or shipping/warehousing function, prepare fraudulent packing slip, authorizes shipment of targeted inventory, delivered to perp, accomplice, or mail drop, fake sales may be created to support shipment, receivable eventually gets written off.

1. **How can employees misuse assets?  What are the "easiest" ways?**
	1. “Borrowing” company assets
		1. company vehicles
		2. supplies
		3. computers and office equipment
	2. results in lost productivity, increased wear on equipment, etc
2. **What are ways that inventory larceny can occur?  When inventory is missing it is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?  How can this missing inventory be hidden?**
	1. Employees take inventory
	2. Shrinkage?
	3. Hidden: financial statements are adjusted, inventory is fake, move inventory between locations
3. **Who is involved and at what times do most inventory larcenies occur?**
	* 1. Involved: employees of the company. Typically, they’re college-educated white males.
		2. What times: towards the end of the period
4. **What are some countermeasures that might assist in reducing losses from inventory larceny?**
	* 1. Check financial statements towards the end of the period for any inconsistencies.
		2. If something seems amiss, track down the source of the problem in question, and investigate further (interviews with involved parties would be a good first step).
		3. Make sure that good internal controls are in place and enforced.
		4. If an employee commits fraud and is caught, the company must prosecute them in order to send a message to would-be fraudsters in the future.
5. **Explain why the following circumstances might indicate that one or more employees are stealing merchandise:**
	1. An increase in uncollectable sales from previous periods, and
		1. If sales are listed as uncollectable when they are not, it would allow a fraudster access to these funds.
	2. An increase in damaged or obsolete inventory from previous periods
		1. An employee could be putting perfectly good items in damaged inventory. Those items will be written off, and the sales revenue that is tied to those items will be written off with the items, allowing the fraudster access to this money.

**Chapter 10/11:**

"Google "conflicts of interest", "bribery", and other topics we are discussing today.  Be ready to discuss in class what you found.

**Conflicts of interest** – occurs when an [individual](http://en.wikipedia.org/wiki/Individual) or [organization](http://en.wikipedia.org/wiki/Organization) is involved in multiple interests, one of which could *possibly* corrupt the motivation for an act in the other.

**Bribery** – payments or other types of compensation made in order to influence and gain profit from an individual or company.
**The "Big Dig" in Boston.**

**What was this project?**

The **Big Dig** is the project that re-routed the chief highway through the heart of Boston, into a 3.5 mile (5.6 km) tunnel under the city.

**What were the original cost estimates?**

$2.8 billion

**What was the final cost?**

$22 billion (with interest) as of 2008

**In the "Spectrum Game" what types of strategies are companies using to gain a competitive advantage?**

1 . Encumber a portion of the spectrum with obligations that will drive down its value and make it less attractive to larger would-be bidders like Verizon, AT&T.

2. Cut off 30% of the spectrum and make it unavailable to only one company to bid for.

 **Investigate the Qui Tam process.  Where might this be useful?**

Qui tam is a provision of the **Federal Civil False Claims Act** that allows private citizens to file a lawsuit in the name of the U.S. Government charging fraud by government contractors and others who receive or use government funds, and share in any money recovered.

**1) What are the four categories of corruption and how are they different?  How are they trying to accomplish the same thing**?

***Bribery and Kickbacks***Commercial bribery is the offering, giving, receiving or soliciting of anything of value to influence the outcome of a business transaction. It typically is committed by employees such as purchasing agents who have discretion in awarding business to outside vendors.

***Economic Extortion***The flip side of offering or receiving anything of value is demanding it as a condition of awarding business. This is termed “economic extortion.” A typical case involves a corrupt lending officer who demands a kickback in exchange for approving a loan.

***Conflicts of Interest***A conflict of interest occurs when an employee, manager or executive of an organization has an undisclosed personal economic interest in a transaction that adversely affects the company or the shareholders’ interests. As with other types of corruption, these schemes involve the exertion of the insider’s influence to the detriment of the entity.

***Illegal Gratuities***Illegal gratuities are similar to bribery schemes, except that something of value is given to *reward* a business decision, rather than *influence* it. For example, purchasing agents commonly are lavished with expensive vacations and other items when a vendor’s contract is approved.

**2) What are the two classifications of bribery schemes?  How are these used?  How can they be mitigated?**

**(1) Bid Rigging** - Bid or Tender-rigging is the process where an employee improperly influences the awarding of a sale or purchase or construction contract. This can be done by:

(a) them knowledge of the conditions to beat
(b) influencing the decision maker towards the briber's tender

**(2) Kickbacks and secret commissions** - Kickbacks are payments received by the employee from the third party after the influence has resulted in a gain to the other person. These payments are usually given to obtain a favorable decision.

**3) Offering a payment can constitute a bribe, even if the illegal payment is never actually made.  Why?**

Because it is illegal to offer payment to reward or influence someone’s decision (under the FCPA)

**4) What are some characteristics of corrupt employees?**

 -Smaller salary than what he/she spends

**Chapter 12/13:**

**"Google "special purpose entity" and be ready to discuss. Are there "new" ways of doing the same thing?**

 -Legal entity created to fulfill narrow, specific or temporary objectives

 -Typically used by companies to isolate the firm from financial risk (shell companies where liabilities are transferred)

 - VIE is now the term now used by the FASB in place of the older term SPE. Since the crash of Enron, SPE has had a negative connotation. The FASB now prefers the term VIE to depict a special entity in which the developing sponsor may have a varying interest in the financial risk.

**1) In an organization, who is responsible for the fair presentation of the financial statements?**

 -Management (tone at the top!!!)

**2) What is financial statement fraud (FSF)?**

 **-**Financial statement fraud is the deliberate and intentional manipulation of the financial records of a company done with the intent to deceive third parties into believing the false statements accurately depicts the company's financial condition.

**3) Why is FSF often referred to as "cooking the books?"**

* 1. Because it involves the financial statement
	2. Change the numbers
	3. Change an egg from a chicken to scrambled eggs

**4) What part of the process of preparing financial statements (e.g., application of GAAP) allows the books to be "cooked?"**

* 1. Human input
	2. Multiple ways to count inventory (Fifo, lifo, etc.)
	3. Very objectice in choosing method

**5) Who, Why, and How are FSFs committed?**

* 1. Everybody that has access
	2. To deceive, create advantage

**6) Who gets hurt from FSF?**

* 1. Investors
	2. Banks
	3. Everybody

**7) Be ready to discuss the five different ways that FSF can be committed.  For each approach, what are the options to implement the fraud?**

Fictitious revenues

* Fabricating revenue
* Inadequate provisions for sales and returns
* Sales with conditions

Timing differences

* Early revenue recognition
* Recording expenses in the wrong period

Concealed liabilities and expenses

* Liability and/or expense omission
* Omission of warranty and product liability

Improper disclosures

* Liability omissions
* Significant events
* Management fraud
* Related-party transactions
* Changes in accounting policy

Improper asset valuations

* Inventory
* Accounts receivable
* Fixed assets
* Business combinations

**\*\*What are some fraud risk factors?  What should you be looking for in an assessment of potential fraud?**

* 1. Lack of separation of duties
	2. Manual entries
	3. “Repo 105”
	4. Lack of disclosures
	5. Consignment
1. **During the audit of financial statements, an auditor discovers that financial statements might be materially misstated due to the existence of fraud. Be prepared to discuss:**
	* **The auditor’s responsibility according to SAS No. 99, the PCAOB, and SOX for discovering FSF;**
		+ SAS No. 99 🡪
			- “The auditor has the responsibility “to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatements, whether caused by error or fraud” (AICPA 2002, pg.3). Based on this standard, the auditor must assess the risk of fraud based on interpretations of this standard and make judgments about the likelihood that there could be material misstatement caused by fraud.”
			- “The audit team must discuss the potential for a material misstatement in the financial statements due to fraud before or during the information gathering process.”
				* Brainstorming!!
		+ PCAOB 🡪
			- “The auditor should evaluate all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company’s financial statements. These controls may be a part of any of the five components of internal control (COSO) over financial reporting, as discussed in paragraph 49. Controls related to the prevention and detection of fraud often have a pervasive effect on the risk of fraud.”
		+ SOX 🡪
			- **SARBANES-OXLEY WILL MEAN BIG CHANGES FOR BOTH** auditors and the companies they audit. The former now will be required to certify a company’s internal controls and will no longer be able to use certain common audit strategies. Management faces the cost of implementing the new rules.
			- **THE AUDITOR MUST ATTEST TO MANAGEMENT’S** assessment of the effectiveness of an entity’s internal controls using standards the Public Company Accounting Oversight Board issues or adopts. The auditor will require management to identify, document and evaluate significant internal controls—management cannot delegate this function to the auditor.
	* **What the auditor should do if she is precluded from applying necessary audit procedures to learn more about and document the suspected FSF;**
		+ There are many ways to obtain information about suspected FSF, if clients are not cooperating go to upper management and beyond.
			- If compliance is still an issue drop the client, they can find someone else to take on their audit.
		+ SAS no. 99 significantly expands the number of information sources for identifying risks of fraud. It provides guidance on obtaining information from
			- Management and others within the organization.
			- Analytical procedures.
			- Consideration of fraud risk factors.
			- Other sources.
		+ ***Management.*** The new standard lists several items you should ask about that relate to management’s awareness and understanding of fraud, fraud risks and the steps taken to mitigate risks. Several of these inquiries were not required under previous standards. Some inquiries are relatively straightforward, but others may require you to “educate” management about the characteristics of fraud, the nature of fraud risks and the types of programs and controls that will deter and detect fraud. The guidance contained in SAS no. 99 provides you with the background necessary to discuss these matters.
		+ ***Others.*** The SAS requires you to make inquiries of the audit committee (even if it is not active), internal audit personnel (if applicable) and others about the existence or suspicion of fraud and to inquire as to each individual’s views about the risks of fraud. “Others” can include those employees who are outside the financial reporting process.
		+ For the most part, auditors tend to restrict their client inquiries to personnel directly involved in the financial-reporting process. This approach is appropriate for matters of which accounting personnel have direct knowledge—for example, how transactions are processed or controlled. However, it is less effective to ask accounting personnel about matters of which they do not have first-hand knowledge (for example, the procedures used to examine, count and receive items into inventory). Critics of the audit process frequently cite the auditor’s reluctance to make inquiries outside of the accounting department as a reason for the lack of the in-depth understanding necessary to plan and perform an effective and efficient audit. SAS no. 99 is the first standard that requires auditors to make inquiries of “others within the entity,” such as
			- Operating personnel not directly involved in the financial-reporting process.
			- People with knowledge of complex or unusual transactions.
			- In-house legal counsel.
				* Further, you should not restrict your inquiries to senior management. The standard suggests making inquiries of personnel at various levels within the organization. These are two primary objectives in making such inquiries.
		+ ***To obtain first-hand knowledge of fraud.*** Fraud can happen in any department and at any level within the organization. Someone in the entity may have observed a person committing or concealing a fraud. Often, those with knowledge of a fraud have stated, after the fact that they would have told someone, “but nobody asked.” SAS no. 99 increases the likelihood that the auditor will now be that “someone” who asks.
		+ ***To corroborate or lend perspective to representations of others.*** Operating personnel can corroborate representations made by others or provide a different perspective on how things “really work.” For example, accounting department personnel may be able to provide you with the recommended control procedures relating to the safeguarding of inventory, but operational personnel can tell you how the control procedures are applied in practice and when, if ever, those controls are overridden or circumvented.
		+ The standard allows you to use considerable judgment in determining to which employees within the organization you should direct your inquiries and what questions you should ask.
		+ **EVEN MORE INQUIRIES**The new standard obligates you to inquire of management and others in the entity. However, it does not restrict you to making only those inquiries. In fact, it encourages you to make additional inquiries in order to gather or corroborate a wide variety of information that can help you identify or assess risks of material misstatement due to fraud. Many of the queries related to these matters should be submitted to personnel outside of management or the accounting department. For example, you may wish to use inquiries to
			- Identify the presence of the fraud triangle characteristics.
			- Understand the policies, procedures and controls for recording journal entries or other adjustments.
			- Identify circumstances under which management has or may override internal controls.
			- Understand policies and procedures related to revenue recognition.
			- Understand the business rationale for significant unusual transactions.
		+ Asking the same question of different people can increase the effectiveness of your inquiries, as you can compare answers to identify consistencies or anomalies in the responses.
	* **What the auditor should do if he finds that the fraud material affects the integrity of the financial statements.**
		+ Tell upper management
		+ Or board
		+ If they don’t address/report the fraud to the SEC in a timely fashion
		+ The auditor should report the fraud to the SEC
2. **What are the commonly used analytical techniques (ARPs) used for financial statement analysis to detect fraudulent reporting?**
	* ARP: Vertical Analysis
		+ Compares general ledger or financial statement balances to other balances WITHIN the same year
		+ Used in both balance sheet and income statement
		+ Highlights changes in account balances within the year as compared to other years
			- Measuring cost of goods sold as a percentage of sales is a type of income statement vertical analysis
			- Comparing current assets to total assets is a balance sheet vertical analysis
	* ARP: Horizontal Analysis
		+ Compares changes in account balances from YEAR TO YEAR
		+ One year would be used as the base line to calculate the percentage change in accounts
			- Examining the percentage change in accounts payable from year 3 as compared to year 2 and year one- would be a B/S example
			- Examining changes in sales from year 3 to earlier years would be an example of an income statement horizontal analysis
	* Looking for unusual changes
		+ i.e., Sales increase by 10% from year 2 to 3
			- You would expect related accounts like A/R, COGS, CASH, AFDA, BD Exp, etc…to increase by relatively the same percentage.
			- If A/R decreases by 30%...possible red flag!!
3. **What is the concept of professional skepticism?**
	* Don’t assume employees are dishonest
	* Don’t assume they are honest
	* Don’t assume they think like you do or have your same ethical/moral beliefs
	* Don’t accept incomplete answers
	* Be a bulldog!
	* But nice!