
FRAUD IN THE IT
DEPARTMENT:
IMPLICATIONS OF SAS 99

Institute of Internal Auditors
Fraud & Ethics Conference -2003

CS 7-2

PRESENTATION OUTLINE

- Introduction
 - Fraud Challenges in the IT Department
 - Implications of SAS 99 on IT
 - Case Study – How an Internal Audit Detected an IT Department Fraud
 - Questions and Conclusions
-

PRESENTERS

■ Joel Lanz

- Over 22 years of IT risk management experience
- Practicing CPA with prior experience as a Big 5 Partner and an Internal Audit Vice President
- Adjunct Professor at the School of Professional Accountancy, College of Management, C.W. Post Campus of Long Island University.
- CISA, CISSP, CFE, CITP
- Publications

■ Ed Patrisso

- Over 15 years of audit experience both public and private.
 - Vice President and Chief Internal Auditor for \$116 billion international Bank.
 - Managed co-sourced IT audit engagement for multi-billion dollar financial institution with a Big 5 CPA firm.
 - Presenter for New York State Society of CPA's.
-

FRAUD CHALLENGES IN THE INFORMATION TECHNOLOGY DEPARTMENT

HOW IS FRAUD IN THE IT DEPARTMENT DIFFERENT?

■ IT'S THE SAME BECAUSE

- Same categories of occupational fraud
- Same elements of fraud need to exist
 - Incentives/Pressures
 - Opportunities
 - Attitudes/Rationalization

■ IT'S DIFFERENT BECAUSE

- Not focus of fraud “professional literature” and when it is, focus is on information security
 - Highly technical jargon and resources – beyond management capability to supervise or verify
 - Significant reliance (“trust”) on employees, vendors and consultants
 - Large expense item on the income statement
-

IT FRAUD ISSUES DISCUSSED IN OTHER CONFERENCE SESSIONS

- Security Planning
 - Hacking and Computer Fraud
 - Data Mining to Uncover Fraud
 - Software Tools for Fraud Detection
-
- *Although we will not be providing “background” information on these fraud-related topics in this session, we would welcome the opportunity to answer any questions on these topics as they relate to the presentation – especially the case study. We would also welcome the opportunity to discuss any of these issues in further detail after the session.*
-

DO GENERAL CONTROLS (AU 319.45) REVIEWS LOOK FOR IT DEPARTMENT FRAUD?

- “Policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems.”
This commonly includes controls over:
 - ❑ Data Center and Network Operations
 - ❑ System Software Acquisition or Maintenance
 - ❑ Access Security
 - ❑ Application System Acquisition, Development and Maintenance
-

**IMPLICATIONS OF SAS 99 –
 (“CONSIDERATION OF FRAUD
 IN A FINANCIAL STATEMENT
 AUDIT”) ON INFORMATION
 TECHNOLOGY**

BRIEF SUMMARY OF THE SAS

- Describes / characterizes fraud – emphasizing professional skepticism
 - Requires discussion amongst audit personnel regarding the risks of material misstatement due to fraud.
 - Defines methods to obtain information needed to identify risks:
 - Inquiring of management and others within the entity about the risks of fraud.
 - Considering the results of the analytical procedures performed in planning the audit.
 - Considering fraud risk factors.
 - Considering certain other information.
 - Obligates auditors to identify risks that may result in a material misstatement due to fraud
 - Calls for a planned response to the results of the fraud assessment.
 - Provides for continuous evaluation of audit evidence.
 - Addresses the need for communicating with management and the audit committee about fraud.
 - Instructs auditors to continuously document the consideration of fraud
 - Need to consider fraud risk factors
-

IT FRAUD CONSIDERATIONS IN EACH AUDIT

- Brainstorming sessions regarding fraud. How can fraud be committed with IT? How can fraud be committed within the IT department? Has fraud ever been committed using IT? What about within the IT Department?
 - Creation of Unpredictable Audit Tests. The engagement team should test systems, locations, functions and accounts that otherwise might not be tested. The team should design tests that would be unpredictable and unexpected by the client. New tests, new work programs, creativity!
 - Documenting the IT environment with an understanding of how & where fraud can be committed.
 - “KICKING” the system tires will no longer suffice.
-

THREE MAJOR CATEGORIES OF OCCUPATIONAL FRAUD

- Asset Misappropriations
 - Involve the threat of misuse of an organization's assets
- Corruption
 - Wrongful use of influence in a business transaction in order to produce some benefit
- Fraudulent Statements
 - Generally involve falsification of an organization's financial statements

Source: "2002 Report to the Nation" Association of Certified Fraud Examiners

ASSET MISAPPROPRIATION FRAUDS IN THE IT DEPARTMENT

- Billing
 - Expense Reimbursement
 - Check Tampering
 - Register Disbursements
 - Misuse of Inventory
 - Larceny
-

CORRUPTION FRAUDS IN THE IT DEPARTMENT

- Conflicts of Interest
 - Bribery
 - Illegal Gratuities
 - Identity Theft
-

FRAUDULENT STATEMENT FRAUD IN THE IT DEPARTMENT

- Financial
 - Asset Overstatements
 - Asset Understatements
 - Non-Financial
 - Credentials
 - Documents
-

EXAMPLES OF RISK FACTORS (AU 316) THAT CAN IMPACT THE IT DEPARTMENT

- Domination of management by a single person or small group without compensating controls.
 - Inadequate monitoring of controls
 - Known or anticipated future employee layoffs
 - Inventory items that are small in size, of high value, or in high demand
 - Inadequate segregation of duties
 - Lack of complete and timely reconciliations of assets
 - Lack of mandatory vacations
-

CASE STUDY

(or, yes this can really happen in
your organization)

THE FRAUD

- The Vice President of IT was receiving hundreds of thousands of dollars through an elaborate and extensive “kickback” scheme
 - He was doing this through the process of purchasing systems equipment and through the hiring of systems consultants
 - He was also purchasing PC’s, printers, and other system-related supplies for himself and his family with Bank funds.
-

THE AUDIT

The Red Flags

- Twelve out of 15 invoices reviewed within our sample were from the same vendor. This included PC's, servers, cable wires, and service contracts.
 - Three consultants were also being paid through this same vendor. We felt there was no way hiring consultants through a 3rd party could be cost effective.
 - In some cases the equipment purchased was being sent home.
 - Many responses by provided by the VP of IT when questioned did not make sense.
 - We attempted gain our own pricing for the consultants we were paying and found that the phone number on the invoice was not in service.
 - The company was not listed in the yellow pages or through directory assistance. We found the address indicated on the invoices was an apartment building and no one by the name of the vendor had occupied it.
-

THE AUDIT (cont.)

- We learned the vendor “walked” equipment over to the office for the majority of the deliveries and never provided shipping documents.
 - The bank’s inventory of system assets was very vague and impossible to trace to actual equipment based on the information maintained.
 - The **time sheets** used for the consultants were generic, not containing the name of any agency. All consultants were from different agencies yet all used the same generic invoice.
 - The **invoices** used for the consultant’s payment were generic and looked like they could easily be PC generated.
 - A review of the invoices for the past year revealed that they were all in sequential order with no breaks, suggesting either our bank was their only client or we had our own invoice numbering system from the vendor.
-

THE AUDIT (cont.)

- A review of cancelled checks revealed that the checks were in all cases payable to the vendor personally and not the company name on the invoices.
 - The checks were being sent to a PO box across the street from the bank when there were several post offices much closer to the business address of the vendor.
 - We then realized 2 other consultants were being paid through yet another 3rd party vendor.
 - We again could not verify the legitimacy of this second vendor. Again unlisted phone numbers on the invoice, the business address was again a residence, invoices and timesheets were again generic.
-

HOW HE DID IT

- Roughly 80% of the bank's IT equipment and supplies were being purchased through 1 vendor
 - The bank was employing 5 out of 7 consultants through a 3rd party
 - He maintained vague procurement procedures
 - He purposely maintained an ambiguous system asset inventory
 - He never maintained shipping documents
 - He was having Purchase Orders created by his staff for cosmetic purposes only after the equipment was already purchased and received
-

HOW HE DID IT

- He had equipment shipped directly to his home for “home use” and neglected to tag the asset or record it on the asset inventory list
 - He alone approved the vendors
 - He never informed Human Resources if consultants were starting an assignment or being released
 - He was creating vendor invoices to pay the 3rd party for the 5 consultants.
-

HOW HE GOT AWAY WITH IT!

- He was trusted by all levels of management and therefore rarely questioned
 - When he was questioned he was a smooth talker and always indicated he was granted certain authority by senior executives who were no longer with the organization so they could not be questioned.
 - He informed Accounting and other members of local management that he had complete authority given to him by Head Office to purchase systems equipment on behalf of the bank and to hire consultants as needed
-

HOW HE GOT AWAY WITH IT!

- He had full control over finding and hiring consultants
 - He never obtained independent bids from vendors
 - He had very little oversight from the Head Office.
 - He intentionally maintained poor documentation
-

ULTIMATE FINDINGS

- The primary vendor was an associate of the VP of IT.
 - The secondary vendor which, we could not initially substantiate the validity of turned out to be the brother-in-law of the VP of IT.
 - In a 9 month period the bank had paid the primary vendor \$1.1 million and the secondary vendor \$400,000 in expenses for supplies, equipment, and consultants out a total of \$1.9 million total expenses
 - Neither vendor had any other clients.
 - Both vendors “went out of business” immediately upon terminating all business with them.
-

BASIC CONTROL DEFICIENCIES

- No segregation of duties. VP of IT had too much control
 - Human Resources never was never aware of hiring or releasing of IT Consultants
 - The Bank had no centralized purchasing function
 - Purchasing authority was concealed through ambiguous and vague procurement procedures
 - No system for obtaining bids
 - No control for delivery check of assets
 - The bank's approval process for assets focused on correctness of payment rather than actual approval of the actual purchase
 - There was no vendor management procedure in place (I.e. approving vendors, due diligence)
-

BASIC CONTROL DEFICIENCIES

- Poor oversight by the Accounting department.
 - They did not require the necessary standard documentation (Purchase Orders, Shipping documents).
 - They did not require confirmation of the receipt of the asset
 - They did not validate the claims of the VP of IT with his superiors that he did in fact have ‘carte blanche’.
 - They did not question the high level of volume to one vendor.
 - They did not question the checks being made out to an individual.
 - They did not question the mailing of the checks to PO box across from the office.
-

QUESTIONS

Edward Patrisso, Vice President & Chief Auditor

Svenska Handelsbanken, NY, NY

(212) 326-5175

edpa01@handelsbanken.se

Joel Lanz

Joel Lanz, CPA, P.C.

(516) 933-3662

jlanz@joellanzcpa.com
