Liberty Bell Hospital: A Case Study In Employee Information Systems Fraud

Michael K. Lavine, Johns Hopkins University and University of Maryland
Amelia A. Baldwin, (Email: abaldwin@cba.ua.edu), University of Alabama, Huntsville
Charles L. Martin, Jr., (Email: chuck819@comcast.net), Towson University

ABSTRACT

Information systems provide an attractive opportunity for dishonest employees in sensitive job positions to develop and implement a fraudulent scheme. Many different types of technical information systems controls help prevent these situations from occurring and can also detect occurrences after they have happened. However, in some cases, employees are able to circumvent critical segregation of duties. In addition, management of a company may override traditional internal controls in order to achieve business objectives. Overriding internal controls can produce an environment that is conducive to fraud.

Internal auditors with an information systems specialty can often identify red flags prior to fraudulent acts taking place in the organization. This allows an organization to utilize preventive measures to reduce the likelihood of a fraud occurring. In a specific situation where an information system fraud is suspected, internal auditors are often charged with leading the investigation. This case analyzes an employee fraud involving a breakdown of internal information technology and management controls, falsification of business records, and a lack of segregation of duties. This case is designed for use in either an undergraduate auditing, information systems security, accounting ethics, internal auditing, computer ethics or other related class. Its primary purpose is to introduce students to a very common type of employee fraud and to illustrate how professional guidance can be applied in such a situation. While the case is based on a true situation, all identities have been modified to protect each individual's right to privacy.

LIBERTY BELL HOSPITAL: CASE SUMMARY

Liberty Bell Hospital (LBH) is affiliated with a prominent university and medical school, and is a large hospital with a national reputation. LBH has 340 in-patient beds, 420 attending physicians and over 3,000 employees. Most of LBH's key software systems were installed in the early 1990s and have undergone significant upgrades and customizations since that time. Recent regulatory changes, market factors and macroeconomic conditions have resulted in falling annual profits which declined from over $3M in 2000 to just over $1M in 2005. After much downsizing and re-engineering, vendors have complained about slow payments from the accounts payable department. Therefore, the accounts payable department was allowed hire one temporary clerk. Eventually, this clerk was hired as a permanent full-time employee. A few months later, suspicious large cash disbursements were uncovered by the accounts payable manager.

INTRODUCTION

Liberty Bell Hospital (LBH) is large hospital located in Philadelphia, Pennsylvania. Founded in 1912, LBH is affiliated with a prominent university and medical school, and has developed a national reputation for excellence in women and children's health services. The company has 340 in-patient beds with 420 physicians on its medical staff. In 2005, with budgeted revenue of $250M and total assets of approximately $300M, the hospital is able to offer a wide range of medical services to the greater Philadelphia community.

Liberty Bell Hospital is organized on a traditional functional level (see Exhibit 1). It maintains a small internal audit department with two Certified Information Systems Auditors. The hospital has long been the market leader in a number of service lines, such as critical care, ambulatory care, and home health care. However, in recent years, with regulatory changes, increasing competition in the local market, and restrictions on referral services imposed by health maintenance organizations (HMOs), traditional modest annual profits of $3M have deteriorated to just over $1M, from 200 to 2005 respectively. LBH's significant information systems are based on mid-range systems such as AS/400 and TANDEM hardware and client/server technology; most of its key software systems were installed in the early 1990s and have undergone significant upgrades and customizations since that time.

In the spring of 2003, LBH embarked on a dramatic business process re-engineering (BPR) effort. With competitive pressures increasing on healthcare providers, LBH sought to reduce its annual operating costs by $25M or 10 percent of its total operating expenditures. This major initiative was started by LBH's chief executive officer [CEO], Bill Thomas, who sought to change the way the organization viewed its patients, employees, and other stakeholder groups.

To begin this large project, fifteen working groups were formed to review operations in all of LBH's business segments. The major working groups included: finance, information systems, nursing and ancillary services (e.g. laboratory, nuclear medicine, pharmacy, and radiology) and physician services. A variety of employees at different staff levels were selected to serve on the working groups and a three-day orientation and training session was organized by the management consulting firm hired to assist LBH in this project. After these working groups were organized, each group identified specific opportunities to reduce on-going operating costs while simultaneously improving patient care and overall customer service.

The administrative work group initiated a study of the accounts payable department, which had ten employees (see Exhibit 2). At the completion of its study, the administrative work group proposed eliminating two A/P Clerk positions that were no longer necessary due to a decrease in the overall number of medical supply vendors. Although Steve Jones, CPA, controller and Tracy Downs, accounts payable manager opposed the staff reduction, all other stakeholder groups approved the proposal. Jones and Downs objected to reducing accounts payable staff because of general performance concerns and a continuous high turnover rate in the accounts payable department. Ultimately, two full-time accounts payable clerks were eliminated from the finance division's operating budget, resulting in an annual savings of $96,000.

Six months later in November 2002, James Smith, chief financial officer (CFO) began receiving complaints from the hospital's main supply vendors. Vendors were upset that they were not being paid on a timely basis, and as a result, were threatening to stop shipping LBH critical patient care supplies. Smith was already aware of this situation based on periodic reports by Jones indicating that the accounts payable department was unable to process all vendor invoices in accordance with the specified terms of trade (e.g. 2/10, n/30) due to a lack of clerical personnel. This also cost LBH money since the attractive purchase discounts were not taken.

This vendor situation left Smith with very few choices about what type of action to take; unilaterally decided to allow the accounts payable department to hire one temporary clerk. When Tracy Downs, A/P Manager, shared this news with her staff, Sharon Harris, Senior A/P Clerk suggested her son, Matt Harris, who was recently laid off from a similar position at a manufacturing company, would be interested in this position.

CASE SOURCE

This case is based on the practical experience developed by one of the authors while was serving as a Director of Internal Audit for a large healthcare system in the Mid-Atlantic area. This case study was developed for the purpose of sharing a significant personal experience from a 'real world' situation that is applicable to all business organizations. Audit workpapers including: information systems reports, system profiles, transaction audit logs and output documents served as the documentary basis for case development. Although this case study is based on an actual situation, all identities have been modified.

INTERNAL CONTROLS AND RED FLAGS OF FRAUD IN INFORMATION SYSTEMS

When Downs interviewed Matt Harris, she found him to be personable, curious, and very eager to work at the hospital. Immediately, she hired him as a temporary accounts payable clerk without interviewing any other candidates. Since Harris was being hired as a temporary employee, he wasn't required to go through a background investigation; which was one of LBH's standard operating procedures for employees in sensitive positions (i.e. IT, Finance etc.). During a routine audit of the finance division, Alan Walters, Internal Audit Manager casually introduced himself to the Matt Harris. When he discovered that Matt was Sharon Harris's son, he immediately researched the company's policies regarding nepotism. His research found that LBH's general administrative policies prohibited 'members of the same family from working in a sensitive department that would potentially impact the integrity or safekeeping of corporate assets or documents'. The situation in the accounts payable department appeared to conflict with LBH's policies and was considered a red flag, indicating a situational environment which is conducive to a potential fraudulent act. Mr. Walters, therefore, decided to call this important issue to the attention of LBH's senior management.

Mr. Walters requested a meeting with James Smith, CFO to discuss the apparent nepotism issue in the accounts payable department. While Smith indicated that he was aware of the company's policy; he explained why he thought it was in the best interest of the hospital to keep Matt in this job. Walters explained this potential fraud environment to Smith who agreed that the situation was not ideal, but disagreed that Matt Harris be re-assigned to another department. Mr. Smith also felt this would not be acceptable since Sharon Harris, Matt's mother, had long been one of the most dedicated members of the accounts payable department, and had even won numerous Employee of the Month awards during her fifteen years of employment

LBH treated Matt Harris like it did any other independent contractor. Liberty Bell Hospital paid all of its contractors and suppliers through the accounts payable module of its financial information system. When a new vendor was identified it was set-up by either Tracy Downs, accounts payable manager, or Elinor Linz, assistant accounts payable manager, by updating the accounts payable master file with the necessary data to ensure timely and accurate processing. Exhibit One details the system flowchart for this process. Tracy Downs was responsible for reviewing this data file each month for obsolete and inactive vendors, as well as overall data integrity issues (i.e. accuracy, completeness etc.)

During September 2002, within two months of working as an independent contractor, a vacancy developed in the department and Matt Harris was given the opportunity to apply for this permanent, full-time position. Although Matt was no longer an independent contractor, his accounts payable vendor file was not deleted by Tracy Downs or Elinor Linz. With the support of Steven Jones, Controller who commented about Matt's pleasant demeanor and cooperative attitude, Tracy Downs hired Matt again without interviewing anyone else or requesting a background investigation. At this time, Matt began to receive all fringe benefits (e.g. health insurance, vacation pay, disability insurance, etc.) and regular weekly paychecks; which were processed with all other employees using the PeopleSoft system.

FRAUD DISCOVERY

In January 2003, Tracy Downs returned from her annual Christmas holiday in Jamaica to discover some very unsettling information. As part of 'catching up' on her work, Downs scanned the system generated Check Register Reports for the three weeks that she was on vacation. This review identified six cash disbursements totaling $80,000 that had been made to Matt Harris. Ms. Downs thought that these disbursements looked suspicious and immediately contacted Alan Walters, the company's Internal Audit Manager. At a meeting later that same day, Downs detailed the primary job responsibilities of Mr. Harris and his employment relationship.

Alan Walters began planning an information systems fraud investigation. Copies of relevant information system reports, cancelled checks from the hospital's bank, supporting cash disbursement authorization forms (see Exhibit Three for sample form) were analyzed, and a thorough review of the accounts payable department's operating

procedures was initiated. Consistent with LBH's policies, members of the information systems, human resources and security departments were notified by the Internal Audit Manager that a possible fraud had occurred. This was to inform all management personnel of about the potential disciplinary and legal ramifications.

Walters discovered that Matt Harris appeared to have forged six cash disbursement authorization forms (see Exhibit 3 for sample copy); which contained vendor invoice data (e.g. vendor name, vendor address, invoice number, and invoice amount). Harris then input the data contained on the fraudulent accounting forms into the accounts payable accounting module under his own vendor account. Input controls help ensure that all data is captured in an accurate and efficient manner. Furthermore, while Harris' supervisor was away on vacation, he was assigned responsibility for performing the semi-weekly cash disbursement run. Another key aspect of this fraud involved the printing and mailing of the physical checks to LBH's vendors. In order to accomplish this task, Matt was allowed access to the main safe where pre-signed checks were stored. It was LBH's standard operating procedure to require a second signature on all checks over $15,000. Matt was very savvy. In order to avoid creating suspicion by management, each of the individual checks he processed was for less than $15,000. At the conclusion of the fraud investigation, the preliminary results were discussed with the accounts payable manager, security director, vice-president for human resources and chief executive officer.

Matt Harris was now to be interrogated. Although all facts seemed clear, LBH desired to obtain a confession from Mr. Harris in addition to identifying a motive for the fraud. Mr. Harris was called at his desk and requested to go to a conference room for a meeting to discuss his employee benefits. Alan Walters, internal audit manager, and Theodore Block, security director, conducted the interrogation and presented Matt with the specific facts uncovered during the fraud investigation. Matt was visibly nervous when he entered the conference room. The following is an excerpt of this discussion:

Walters: Matt we called you to this meeting to discuss a very serious matter. I have conducted a fraud investigation surrounding six cash disbursements in your name.

Harris: I don't know what you mean.

Walters: It seems that when your supervisor, Ms. Downs was away on vacation you forged six accounting documents that generated checks to yourself.
<Long Pause>

Block: This is a serious matter and a fraudulent act like this is considered a felony crime in the State of Pennsylvania.

Walters: Our goal here is to confirm the facts and understand your reasons for perpetrating this fraud.
<Long Pause>

Harris: I want you to know…..I did this by myself……I am very ill and have over $50,000 in credit card bills that I incurred to pay for experimental drugs that may possibly cure me.

After a short period of silence Harris began to cry, and later confessed to the crime and explained that he was forced to steal from LBH because he was diagnosed with a terminal illness and had no personal assets or health insurance with which to pay for the treatments. Standard medical treatments had not been successful and experimental treatments, which were not Food and Drug Administration approved, were not available in the United States. Matt had to obtain treatments and medications in Mexico.

When questioned, once again, about the involvement of any other parties, and, in particular, his mother, Mr. Harris reiterated this fraud was solely his doing. He explained to Mr. Walter and Mr. Block how he had already spent the funds he had stolen and did not have a means to make repayment. Matt then signed a written confession, and was immediately suspended without pay.

DISCUSSION QUESTIONS

- What factors contributed to this opportunity to commit fraud?
- What breakdowns in internal control could have been improved so that this fraud could have been prevented?

- Other than Matt Harris, who bears some responsibility for this fraud?
- Did the Alan Walters, Internal Audit Manager do the right thing?
- Explain how general computer controls and application level controls could have helped prevent and detect this fraud?

EPILOGUE

While this situation was very troubling for all personnel involved, everyone felt it was important to do the right thing. The hospital subsequently filed legal action against Mr. Harris seeking felony charges and restitution. While the court case was pending Mr. Harris died. This left LBH unable to recover its $80,000 loss due to a lack of assets in Mr. Harris' estate. Due to this fraud, the Information Systems and Finance Departments worked together to implement the recommendations developed by the Internal Audit Department during the fraud investigation. All of the recommendations were positively received by senior management, and no additional frauds were evident.

CONCLUSION

This case illustrated a variety of risks and corresponding controls that are normally found in a financial information system. It illustrates how a well designed information system, can still have weaknesses in it. Then, once a system weakness is discovered by an employee; he/she can exploit it to take personal advantage. Another important issue brought out in the case is that company management can override policies and procedures at their discretion. While sometimes justified, the corresponding risk needs to be fully understood. Lastly, LBH provides an interesting example of how information systems auditors can work with other employee groups to improve internal controls, governance and protect against future fraudulent activities.

BIBLIOGRAPHY

1. Association of Certified Fraud Examiners. 1998. *Report to the Nation on Occupational Fraud and Abuse.*
2. Bakersville, R. 1993. Information Systems Security Design Methods: Implication for Information Systems Development, *ACM Computing Surveys*, December, pp. 375-414.
3. Comer, M. 1998. *Corporate Fraud*, Third Edition, Gower Publishing Limited, Hampshire, England.
4. Gelinas, U., S. Sutton, and J. Hunton, 2005. *Accounting Information Systems*, Sixth Edition, South-Western College Publishing, Cincinnati, OH.
5. Guy, D., C. D. Alderman, and A. Winters. 2000. *Auditing*, Fifth Edition, Dryden Press, Forth Worth, TX.
6. Information Systems Audit and Control Association. 2003. *CoBIT: Governance, Control and Audit for Information and Related Technology*, Third Edition, Rolling Meadows, IL Available here: http://www.itgovernance.org or http://www.isaca.org.
7. Just, G. R. 1998. Upheaval & Opportunity: Five Risk Laden Areas That Plaque Health Care. *Internal Auditor*, April, Volume LV, Number 11. pp. 40-47.
8. McCarthy, M. and A. Schachter. 1998. *Fraud in the Health Care Industry: The Auditor's Responsibilities Under SAS No. 82*, American Institute of Certified Public Accountants, Jersey City, NJ.
9. Moyes, G. D. and M. K. Lavine. 1997. Fraud: Which Audit Techniques Work in Detecting Fraud?" *Corporate Controller*, Volume 10, Number 6, pp. 43-47.
10. Mullet, K. and Sano, D. 1995. *Designing Visual Interfaces*. Sunsoft Press, Englewood Cliffs, New Jersey.
11. Weber, R. 1999. *Information Systems Control and Audit*, Prentice-Hall, Upper Saddle River, New Jersey.
12. Wells, J., C. Bell, G. Geis, W. M. Kramer, J. Ratley, and J. Robinson. 1993. *Fraud Examiners Manual, Association of Certified Fraud Examiners (ACFE)*. Second Edition, Volumes I and II.
13. Wells, J. T. 2003. The World's Dumbest Fraudsters, *Journal of Accountancy* (May). Available online: http://www.aicpa.org/pubs/jofa/may2003/wells.htm.
14. Whitten, J. L., Bentley, L. D., and Dittman, K.C. 2004 *Systems Analysis and Design Methods*. Sixth Edition, McGraw/Hill Irwin.
15. Zikmund, Paul. 2003. Ferreting Out Fraud. *Strategic Finance* (April) pp. 28-32.

LIST OF EXHIBITS

- Exhibit One – LBH Overall Organizational Chart
- Exhibit Two – Finance Division Organizational Chart
- Exhibit Three – Authorization for Cash Disbursement Form
- Exhibit Four –Accounts Payable Module System Flowchart

Note: Permission is granted for all items to be modified in terms of content and file format as needed by the editors and adaptors of this case study. This case study has benefited from classroom discussion and enhancements made based on peer-reviewer feedback from both: two previous conference presentations and one prior journal submission.

Exhibit One – LBH Overall Organizational Chart

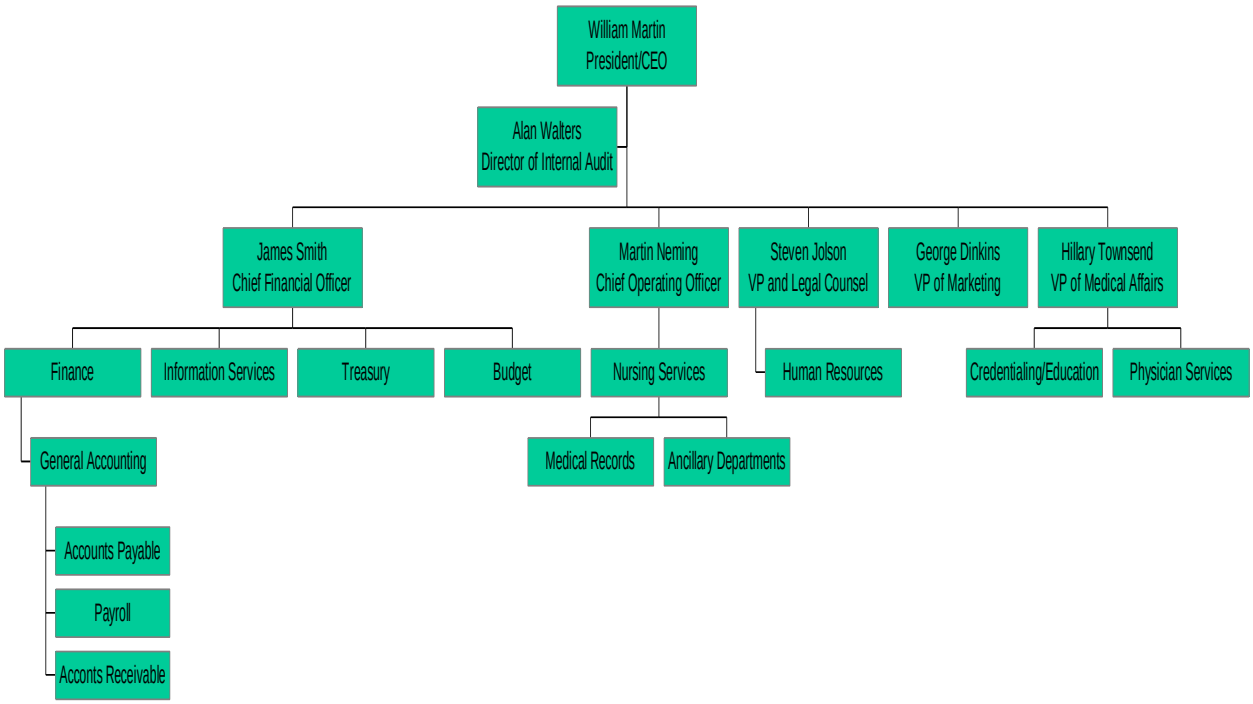

Exhibit Two - Finance Division Organizational Chart

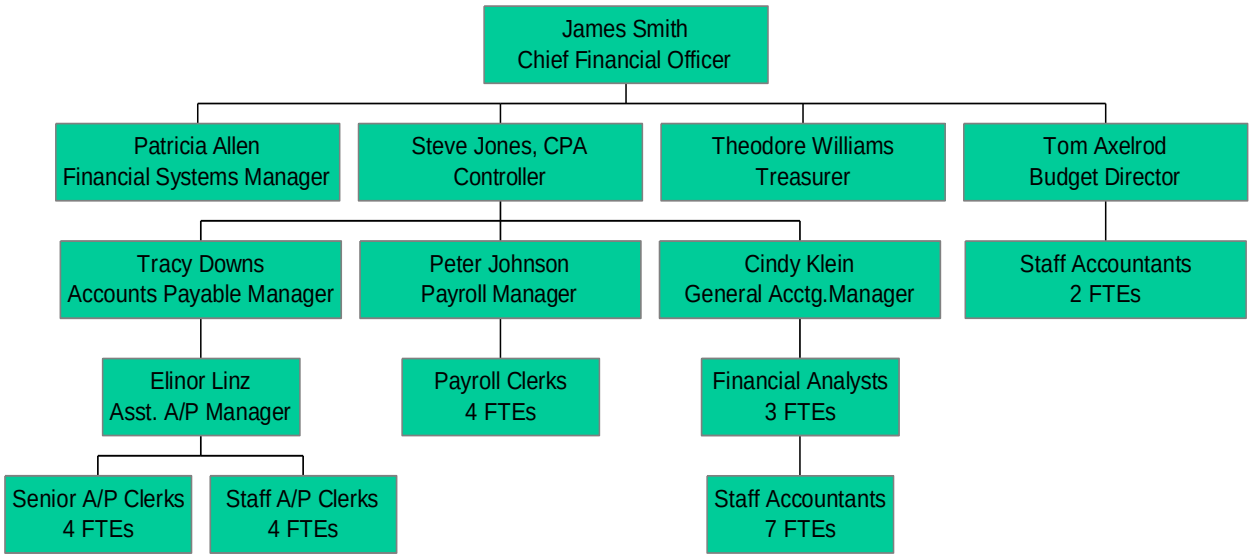

Exhibit Three – Authorization for Cash Disbursement Form

LIBERTY BELL HOSPITAL, INC.
AUTHORIZATION FOR CASH DISBURSEMENT

Date: _____

Pay to the Order of: _____

Street Address: _____

City: _____

State: _____

Zip Code: _____

Dollar Amount: _____

_____
Authorized Signature

Invoice Number: _____ Invoice Date: _____

G/L Account Number: _____ Three Digit Department Number: _____

Input By: _____ A/P Voucher Reference: _____

Form No. LBH314 Last Revised: 2/13/03

TEACHING NOTES

Magnitude of Occupational Fraud and Abuse

The Association of Certified Fraud Examiners defines occupational fraud and abuse as "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets." Based on a two and a half year study, the association found that:

- The average organization loses more than $9 a day per employee to fraud and abuse;
- The average organization loses about 6 percent of its total annual revenue to fraud and abuse committed by its own employees;
- Fraud and abuse costs U.S. organizations more than $400B annually; and
- The median loss per case caused by males and females is about $185,000 and $48,000, respectively.

The data indicates that about 58 percent of the reported fraud and abuse cases were committed by non-managerial employees, 30 percent by managers, and 12 percent by owner/executives. The median loss by non-managerial employees ($60,000) was significantly less those caused by managers ($250,000) and executives ($1,000,000), respectively.

The study found that smaller organizations are the most vulnerable to occupational fraud and abuse. Organizations with one hundred or fewer employees suffered the largest median losses per capita. Generally, this is because sophisticated controls, designed to deter occupational fraud, are less prevalent in smaller organizations.

The study also found that relatively few occupational fraud and abuse offenses are discovered through routine audits. Most fraud is uncovered as a result of tips and complaints from other employees. To deter and detect fraud and abuse, many experts believe an employee hotline is the single most cost-effective measure. The study concluded with an ominous prediction that the rate of occupational fraud and abuse will likely rise due to many complex sociological factors. Among other things, increasing demands on the criminal justice system by violent criminals may make fraud and abuse prosecutions more difficult. Additional proactive vigilance and education, as well as consumer action, could stem future increases in occupational fraud and abuse.

Use

This case was designed for use in an undergraduate course in information systems, information systems security, computer ethics, or accounting information systems. Its primary purpose is to introduce students to a common type of employee fraud that can be perpetrated in a financial information system. It also illustrates how technical and other (i.e. management, business process) controls can be utilized to maintain an effective information system. This case can be used to integrate coverage of the auditor's consideration of fraud and internal control.

The case may also be used as a comparison to timely examples of fraud in recent news reports. The roles of an independent internal audit department, for example, in exposing the WorldCom fraud could be used to illustrate the magnitude of fraud the internal auditors may uncover using information systems audit tools. As well, how this business unit can support the information systems operations are also included in this case study. This case may also be used as an illustrative example to enlighten discussion of CObIT [Control Objectives for Information and related Technology] which was developed by the Information Systems Audit and Control Association as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference model for management, users, and IS audit, control and security practitioners.

Behavioral Learning Objectives

- The case can be used to assess student performance involving two learning objectives:
- Ability to identify fraud risk factors in information system; and
- Ability to identify related internal controls and the weaknesses thereof.

Case Development

This case is based on the work experience developed by one of the authors while was serving as a Director of Internal Audit for a large healthcare system. The actual audit work papers served as the documentary basis for case development. Although this case study is based on an actual situation, all identities have been modified to protect each individual's privacy.

Notes on Discussion Questions

The following notes may be used to guide student discussion of the end-of-case questions. The notes are not meant to be all-inclusive.

1. What factors contributed to this opportunity to commit fraud?

In this case, numerous risk factors relating to controls were present. Specifically,

- Lack of appropriate management oversight (inadequate supervision with too many key personnel on vacation simultaneously and not purging the A/P master file)
- Lack of applying established job applicant screening procedures (need for expediency and ignoring established policy on nepotism)
- Lack of appropriate segregation of duties (access to C/D authorization forms and pre-signed checks)
- Lack of appropriate system for authorization and approval of transactions (breakdown during vacation)

2. What breakdowns in internal control could have been improved so that this fraud could have been prevented?

Following established organizational policies, especially at the initial stage of the hiring process could have prevented this fraud. Although Liberty Bell Hospital had established guidelines for hiring, they were not followed due to the need for expediency and in order not to alienate a loyal employee. By following the established guidelines, Matt Harris would never have been considered since he was related to another employee in the same department. Even if Matt were hired, a required background check (including credit history) would have discovered his financial predicament (i.e. high credit card debts, gaps in employment history). The fraud could have been detected earlier if someone else who had no control or authorization over the A/P system, such as the Accounting Manager, reviewed the check registers for unusual transactions.

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. In this case, James Smith, CFO, circumvented the company's nepotism policy and ignored the warnings of Alan Waters, Manager of Internal Audit. Mr. Smith's actions mitigated the control consciousness of the organization, thereby jeopardizing the overall control environment. Additionally, Tracy Downs, A/P Manager, circumvention of Matt's background check also jeopardized the control environment. Adherence to company policy would have alleviated these problems.

Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or irregularities in the normal course of his/her duties. In this case, Matt's duties

changed while his supervisor was on vacation. Since his vendor account was not purged from the A/P master file, he now had custodial, authorization, and record-keeping duties. This placed him in a position to authorize payments to himself, physically issue checks to the himself, and record the transactions. Matt's vendor account should have been inactivated or deleted on the financial information system, so he could no longer be able to enter this information onto his vendor account. Furthermore, he also should not have had access to the pre-signed checks in the main safe.

Physical security of assets, including adequate safeguards over access, should be maintained. Although the hospital has a secured safe in which to store the pre-signed checks, the checks should never have been pre-signed; thereby, making them negotiable. Additionally, a recently hired employee should be not permitted access to the safe. Another area of concern relates to Matt and his mother working in the same department. Although they have different functions, being close relatives, their segregation of duties could have been circumvented by collusion. Once again by following company policy and assigning them to different departments, this problem could have been avoided.

According to the case Liberty Bell Hospital apparently does not have a policy of investigating the criminal background of temporary employees. This may be due to employment of temporary personnel through an employment service agency with the expectation that the service-company investigates the individual's background. Liberty Bell Hospital should require criminal background investigations of all employees, whether temporary or permanent, whether hired directly or through an employment agency.

3. Other than Matt Harris, who bears some responsible for this fraud?

Although Matt perpetrated the fraud and is directly responsible for this situation to commit this fraudulent act would not have existed if James Smith didn't ignore the nepotism issue. Similarly, Tracy Downs could have helped avoid this fraud if she had insisted that a background investigation be performed before Matt was hired as a contractor or when he became a regular hospital employee.

4. Did the Alan Walters, Internal Audit Manager do the right thing?

Even though there is empathy for Matt's plight, Alan Walters, the Internal Audit Manager, discharged his duties properly.

5. Explain how general computer controls and application level controls could have helped prevent and detect this fraud?

According to COBIT, control is defined as: "The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected." IT Control Objective is defined as: "A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity." IT Governance is defined as: "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes." Where did the breakdown occur in this instance? Clearly in IT governance, because for the most part the appropriate policies existed but were not followed.

Concerning COBIT control process domains, the major weak area that contributed most to the resulting fraud was *planning and organization*. The problem is not just at the point of the perpetrator's actions, but part and parcel of the planning and organization processes that allowed existing controls to be subverted or ignored. Some preventive controls existed, but were circumvented by managers.

Concerning the critical failure of a specific COBIT detailed control objective, segregation of duties (or lack thereof) is a major factor here. Planning and organization (control process domain) detailed control objective for segregation of duties, *4.10*, requires not only that single employees be unable to subvert a critical process, but also that they should only be able to perform the duties that are assigned to their respective job. Clearly, the subversion of hiring and job assignment controls allowed a critical failure in segregation of duties.