THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 1 | Number 1 Article 2

2006

AlphaCo: A Teaching Case on Information Technology Audit and Security

Hüseyin Tanriverdi
The University of Texas at Austin

Joshua Bertsch
The University of Texas at Austin

Jonathan Harrison
KPMG, LLP

Po-Ling Hsiao
The Walt Disney Company

Ketan S. Mesuria
Ernst & Young, LLP

See next page for additional authors

Recommended Citation

Tanriverdi, Hüseyin; Bertsch, Joshua; Harrison, Jonathan; Hsiao, Po-Ling; Mesuria, Ketan S.; and Hendrawirawan, David (2006) "AlphaCo: A Teaching Case on Information Technology Audit and Security," *Journal of Digital Forensics, Security and Law*: Vol. 1 : No. 1 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2006.1001
Available at: https://commons.erau.edu/jdfsl/vol1/iss1/2

AlphaCo: A Teaching Case on Information Technology Audit and Security

Authors

Hüseyin Tanriverdi, Joshua Bertsch, Jonathan Harrison, Po-Ling Hsiao, Ketan S. Mesuria, and David Hendrawirawan

AlphaCo: A Teaching Case on Information Technology Audit and Security[1]

Hüseyin Tanriverdi
McCombs School of Business
The University of Texas at Austin
Austin, Texas 78712-0212 USA
Huseyin.Tanriverdi@
mccombs.utexas.edu

Joshua Bertsch
The University of Texas at Austin
Austin, Texas 78712-0212 USA
jbertsch@mail.utexas.edu

Jonathan Harrison
KPMG, LLP
Houston, Texas 77002 USA
jonathanharrison@kpmg.com

Po-Ling Hsiao
The Walt Disney Company
Burbank CA 91521 USA
Po-Ling.X.Hsiao.-ND
@disney.com

Ketan S. Mesuria
Ernst & Young, LLP
Dallas, TX 75201 USA
Ketan.Mesuria@ey.com

David Hendrawirawan
Deloitte & Touche LLP
Houston, TX 77002 USA
dhendrawirawan@deloitte.com

ABSTRACT

Recent regulations in the United States (U.S.) such as the Sarbanes-Oxley Act of 2002 require top management of a public firm to provide reasonable assurance that they institute internal controls that minimize risks over the firm's operations and financial reporting. External auditors are required to attest to the management's assertions over the effectiveness of those internal controls. As firms rely more on information technology (IT) in conducting business, they also become more vulnerable to IT related risks. IT is critical for initiating, recording, processing, summarizing and reporting accurate financial

[1] AlphaCo is a fictitious company. The purpose of this teaching case is to serve as a basis for classroom discussions rather than to illustrate effective or ineffective handling of IT audit and security issues. Hypothetical facts and scenarios are used to enrich classroom discussions. Resemblance to any real company is unintentional. The teaching case is prepared by Joshua Bertsch, Jonathan Harrison, Poling Hsiao, and Ketan Mesuria as part of their student team project in the IT Audit & Security Course at the Red McCombs Business School. The project was completed under the professional guidance of David Hendrawirawan and the academic supervision of Professor Hüseyin Tanriverdi. The project won the Best Student Project Award of the Austin Chapter of ISACA during the 2005 spring semester.

and non-financial data. Thus, understanding IT related risks and instituting internal control mechanisms that minimize them have become important and created an urgent need for professionals who are equipped with IT audit and security skills and knowledge. However, there is severe shortage of teaching cases that can be used in courses aimed at training such professionals. This teaching case begins to address this gap by fostering classroom discussions around IT audit and security issues. It revolves around a hacking incident that compromised online order processing systems of AlphaCo and led to some fraudulent activity. The hacking incident raises a series of questions about IT security vulnerabilities, internal control deficiencies, integrity of financial statements, and independent auditors' assessment of fraud in the context of the Sarbanes-Oxley Act. The case places students in the roles of executives, IT managers, and auditors and encourages them to discuss several important questions: how and why did the hacking incident happen; what harm did it cause to the firm; how can the firm prevent such hacking incidents in the future; if they do happen, how can the firm detect hacking incidents and fraud sooner; how do auditors assess the impact of such incidents in the context of a financial statement audit; and whether the management and auditors have responsibility in detecting and publicly reporting fraud? The case also facilitates the teaching of relevant conceptual frameworks such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) and COBIT (Control Objectives for Information and related Technology).

Keywords: Information technology, risk, internal control, security, hacking, audit, fraud, financial reporting, compliance, Sarbanes-Oxley Act, teaching case

1. INTRODUCTION

In early 2002, the accounts receivable department of AlphaCo discovered a significant amount of uncollected accounts while performing an aging analysis. These accounts totaled in the millions and were tracked to shipments to an Aegean Island. Several of the accounts were listed under the same address. Further reviews revealed that the accounts were fraudulent. A hacker penetrated the online order management system of the firm, created fake accounts and placed about 50 fraudulent orders over a period of three months and stole shipments that have a value of approximately $20 million.

When they called the phone number listed in the fraudulent accounts, to their surprise, AlphaCo representatives were able to reach the hacker, who seemed to be waiting for the AlphaCo's call. The hacker threatened that unless the firm paid him $10 million, he would publish IT security vulnerabilities of the firm and his hacking techniques on the Internet and harm AlphaCo's reputation. AlphaCo immediately contacted law enforcement agencies. In recent years, these kinds of hacking incidents and extortions were on the rise. Several international hackers compromised computers throughout the United States

and stole usernames, passwords, credit card information, and other financial data, and then extorted the victims with the threat of deleting their data and destroying their computer systems. Thus, the law enforcement agencies viewed this as a serious crime and a major threat to electronic commerce and the integrity of data that the financial community relies upon to do business nationally and internationally.

With the knowledge of the law enforcement agencies, AlphaCo entered negotiations with the hacker. While the effort to catch the hacker was underway, AlphaCo brought in computer forensics experts and IT security consultants to investigate how exactly the online order management system had been breached. This information was crucial for fixing the IT security vulnerabilities that allowed the hacking incident and also for preparing electronic evidence to present to the courts to prosecute the hacker once he is caught. After their initial investigation, the computer forensics experts reported that it would be a very costly effort to find, capture, and preserve the electronic evidence left by the hacker and to prepare the evidence for the court case.

The Chief Information Officer (CIO) called the Chief Executive Officer (CEO), Chief Financial Officer (CFO), and the Director of Internal Audit (DIA) into an urgent meeting. The CIO informed the top management that the firm's business relies heavily on IT and that the breach of security in the online order management system can cause significant harm to the firm's reputation and business. He urged the top management to increase the IT budget significantly so that they can undertake a full computer forensics investigation to identify and fix the IT security vulnerabilities of the firm. He also emphasized how important it is to use professional computer forensics expertise in capturing, preserving and preparing the electronic evidence to be able to prosecute the hacker in the court of law.

Standing in stark opposition to the CIO's request was the CFO, who wanted the IT department to adhere strictly to its original budget and solve any problems within the constraints of the budget. The CFO explained that the firm's IT budget was already significantly above the industry average. The CEO sympathized with the CFO. He was worried that increasing the IT budget further could increase the cost of doing business significantly. The CEO and CFO were questioning whether further investments into IT security were really necessary.

The Director of Internal Audit (DIA) touched on another important implication of the hacking incident. She explained that the section 302 of the newly introduced Sarbanes-Oxley (SOX) Act of 2002 requires the CEO and CFO of a public company to certify quarterly and annually that they are responsible for disclosure controls, they have designed controls to ensure that material information is known to them, evaluated the effectiveness of controls, presented their conclusions in the filing, and disclosed to the audit committee

and auditors significant control deficiencies and acts of fraud. Further, section 404 of SOX requires the CEO and CFO to annually state their responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting, conduct and provide an assessment of the effectiveness of the enterprise's internal controls. It also requires the external auditor to attest to the management's assertion and the internal controls identified by the management. In the short-term, she was concerned that the fraudulent orders of the hacker could have an impact on the firm's financial statement audit. In the long-term, she anticipated that these kinds of IT security breaches could inhibit the firm's ability to comply with SOX. She informed the CEO and CFO that her department recently adopted the COSO[2] and COBIT[3] frameworks, which are among the state of the art conceptual frameworks for thinking about internal controls around the firm's business processes and the supporting IT systems. But she emphasized that her department will also need a significantly increased budget to implement the internal control best practices implied by those frameworks.

The DIA's explanations changed the course of the discussions. The CEO and CFO began asking questions about how SOX requirements and COSO and COBIT frameworks inform issues pertaining to the hacking incident. They were worried about the potential impact of this incident on the firm's financial statement audit and the firm's ability to comply with SOX. They also wondered whether the firm should disclose the hacking incident publicly.

2. ALPHACO BACKGROUND

AlphaCo Inc. is a global distributor of a diversified range of mechanical, electrical, and electronic systems and components such as semiconductors, liquid crystal displays, data communications equipment and supplies, electromechanical devices, mechanical and electrical power transmission products, bearings, conveyor components, electric motors, industrial computer products and subsystems, and so forth. In addition, it offers a complementary set of services to its suppliers and resellers such as financial services, logistics, sales, marketing, engineering, and customer support. AlphaCo operates in 150 countries across Africa, Asia, Eurasia, Europe, Australia, North America and South America. It has 105 distribution centers worldwide and sales offices or representatives in 95 countries. The firm is headquartered in the U.S and

[2] COSO stands for The Committee of Sponsoring Organizations of the Treadway Commission. This committee was formed in 1985 to study causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. The COSO framework is the result of those studies.

[3] COBIT stands for Control Objectives for Information and related Technology. It is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

publicly traded in the New York Stock Exchange. Since it has presence worldwide, it is subject to not only the U.S laws and regulations, but also the laws and regulations of the markets in which it operates.

AlphaCo operates in a highly competitive environment worldwide. It does business with manufacturers, distributors, and resellers who sell directly to end-users. AlphaCo has a very diverse product line. It markets and distributes more than 500,000 products from over 5000 suppliers. Its global presence provides suppliers with access to a broad base of geographically dispersed resellers. The diverse product line enables the firm to serve as a one-stop shop for many customers. The ability to cross-sell multiple products to the same customer increases revenues of the firm. The global reach and diverse product line of the firm also minimize the firm's exposure to economic downturns. Even when some product lines and markets experience downturns, the firm is able to smooth out its cash flows by relying on other product lines and markets in its portfolio. In 2002, net sales of the firm exceeded $42 billion (See Appendix 1).

To provide quick order taking and fulfillment capabilities and consistent, timely and accurate delivery around the world, AlphaCo invested heavily in IT. The core IT infrastructure of the firm relies on mainframes. But it also includes a variety of IT hardware and operating system platforms that were inherited from mergers and acquisitions of the firm over the years. AlphaCo is one of the earliest adopters of enterprise resource planning (ERP) systems and e-business capabilities. Recently, it made several investments to better integrate its modern and legacy systems and build web-based interfaces to provide access to customers and business partners. AlphaCo employs about 1500 IT staff worldwide to support its IT infrastructure. The IT infrastructure processes more than 20 million business transactions per day. It is designed to provide speed, reliability, fault tolerance, and extra bandwidth, storage and processing capacity to accommodate annual growth rates of 50%.

3. ORDER MANAGEMENT SYSTEM

AlphaCo's order management system provides service to manufacturers and resellers via the internet. It acts as a channel middle man between manufacturers and resellers. The company's business dependency on the World Wide Web requires maintaining assurance around the integrity of transactions. To address the security threats posed by e-commerce, AlphaCo uses Secured Socket Layer (SSL), which provides 128-bit encryption of packets to and from its e-commerce clients. Furthermore, all manufacturers and resellers are required to authenticate themselves as legitimate business partners. This process is very rigorous, as authenticated resellers can receive discounted products and create lines of credit. After a reseller is approved and given an online account, proof of sales of $5000 or more is expected within 60 days, or a probationary period begins. The probationary period escalates to termination

of an account if proof of sales is not shown within 120 days. Once resellers log on to AlphaCo's order management system they are able to purchase products for reselling. When an order is made, a shipping order is placed in the shipping database. At AlphaCo's warehouse, a distribution associate ships out the order and creates an invoice in the billing database. A billing agent processes the invoice to determine whether it should be mailed to the client or withdrawn directly from the client's bank account. A mailed invoice is entered into the collections database. When an invoice is not paid within 90 days it is written off as a bad debt. An unpaid invoice under $1500 places the user account on a probationary period while an uncollected invoice exceeding $1500 results in the termination of the user account. The second occurrence of non-payment results in the termination of the user account (see Appendices 2 and 3).

4. ALPHACO RESPONSE

The CIO was disappointed with the fact that AlphaCo had been hacked. But he was particularly concerned with the fact that it took the firm three months to detect the hacking incident. While the CEO and CFO were considering the CIO's request for additional IT budget, the CIO had to respond to the potential IT security vulnerabilities immediately within the constraints of his current budget.

Working with what they already know, the IT department, computer forensics experts, and IT security consultants constructed a preliminary scenario about how the hacking might have happened. They reasoned that the hacker initially penetrated AlphaCo's online system by exploiting an unpatched service running on an exposed web server. The exploit gave the hacker root access, which was used to view connection strings to the order management system's database. The database resided within AlphaCo's internal network. Using the database connection strings and spoofing web server identity, the hacker was able to connect to the database and execute SQL statements. At that point the hacker had the ability to create fake accounts from which to place the fraudulent orders. The network penetration did not stop there. Through the database, extended stored procedures were used to discover yet another unpatched service and install password sniffers[4], which were used to create unauthorized Virtual private network (VPN) connections. A reverse tunnel was created using the exploited service, thus connecting the database server to the hacker's local workstation. The database server was then used as a proxy to discover other critical servers on the network and the services they owned.

Despite the plausibility of the preliminary scenario, both the consultants and the IT department acknowledged that there could be alternative scenarios explaining the hacking incident. A costly computer forensics investigation of

[4] "Password sniffers" are applications used to discover passwords by scanning cached data, capturing key strokes, or decrypting encrypted data.

the available electronic evidence was necessary to discover how exactly the hacking incident happened. But nobody was sure if the evidence remained intact since the hacking incident.

Patch management was the first item identified as lacking. All critical servers needed to be up to date with critical patches within 72 hours of patch release. The next item was creating a policy that required all database connection strings to be encrypted. In reaction to the potential for installation of password sniffers, virus scanning software was upgraded on all critical servers and configured to receive automatic updates of new malicious software to scan for. Also, all software on critical servers needed to have a business justification for being installed.

Several monitoring controls were put in place to detect fraud. All new customer accounts were to be reconciled each month for appropriate credit check approval. Also, security logs and virus scanning logs were to be reviewed each week for possible network intrusions. Other areas identified as lacking controls were firewalls and account administration. Firewall configurations needed to be appropriate and open ports needed to be justified. Also, generic accounts and administrative accounts without business justification needed to be removed from critical servers. This would not only benefit account administration, but also increase the transparency of the security logs.

Despite these measures, the CIO was wondering what else they need to do to prevent hacking attempts, and to detect an incident sooner if hackers manage to compromise their systems again in the future. The IT security consultants who reviewed the initial response of AlphaCo praised the IT department in addressing technical vulnerabilities. But they also recommended the development of a more comprehensive policy that addresses all relevant dimensions of IT security.

5. AUDITOR RESPONSE

After the internal investigation, AlphaCo informed its external auditor about the hacking incident. The external auditors called for several meetings with the management to discuss the case. After the meetings, the audit senior managers and partners engaged in a discussion to determine whether and how this hacking incident would affect the financial statement audit. They documented their thought process and rationale in a question and answer format as follows:

1. *What is the control activity that* failed *in this incident?*
   The network security controls for the online ordering system appeared to have been lacking, as demonstrated by the successful intrusion by a malicious hacker.
2. *Is this an indication of* pervasive *control weakness?*
   No. We have tested other General Computer Controls, including

Information Security controls at the Network, Operating System, Database, and Application layers. Our test of controls did not indicate any significant issue with the Information Security control environment.

3. *What is the* likelihood *that similar incident would occur in the future?*
   It would be difficult to answer this question with certainty, but according to the professional judgment of our IT Security Specialists, the technique employed by the hacker is relatively high in sophistication and rigor. In other words, it is not something that can easily be re-performed.

4. *What are the* actual AND maximum potential *loss and/or misstatement resulting from the control failure?*
   The actual loss from this known event alone was $20 million. Based on professional judgment, we estimate that there could be no more than 10 other incidents occurring throughout the fiscal year, either detected or not. As such the total potential misstatement for the entire fiscal year is $200 million overstatement of Accounts Receivable and Revenue balances.

5. *Is there any* redundant or compensating control *that could prevent or detect potential future violations?*
   This incident was discovered by the company due to their Accounts Receivable Aging Review process. The Accounting department reviews all A/R balances that have been outstanding for a certain period of time. For example, any balance older than 90 days are flagged and researched by the Credits and Collections department, who may contact the customer if no satisfactory explanation is available. After 120 days, the balance will be transferred to "Uncollectible Balances". It was through this process that they were able to discover an anomaly with the customer accounts used by the hacker to purport this fraud. By the time the process caught up, the damage was $20 million. By further analysis, we can reasonably say that the compensating control exists to catch any error in the amount of $5 million or more, over a 90 days period. This translates to $20 million per year.

6. *What other* qualitative factors *can be considered in our analysis?*
   The fact that the company was able to catch the misstatement within a reasonable time-frame and prior to the Auditor is indicative of effective *detective* and *corrective* control compensating for weakness in *preventive* control. Since the discovery of the issue, the company had taken steps to improve the information security control environment.

7. *Given all of these considerations, how should we consider the issue and its impact on our audit?*
   Although the company's internal controls could not prevent all fraud, they appear adequate for detecting and correcting one. Apart from making the proper adjustment to reflect the uncollectible balance resulted from this incident, we do not think any further adjustments are necessary. However, we should perform follow up procedure to ensure that the new security measures the company had committed to have been implemented. Furthermore, we should increase the rigor and sample size of our substantive testing on the account balances that could be affected by this incident, namely Accounts Receivable and Revenue from sales. We should also conduct a follow up compliance testing on the compensating controls that were relied upon by the company to detect potential future misstatements from similar incidents (i.e., A/R Aging, Bank Reconciliation, etc.).

6. OUTCOMES

The audited financial report of AlphaCo in 2002 did not make any reference to the hacking incident, the resulting fraudulent activity, or the loss of approximately $20 million.

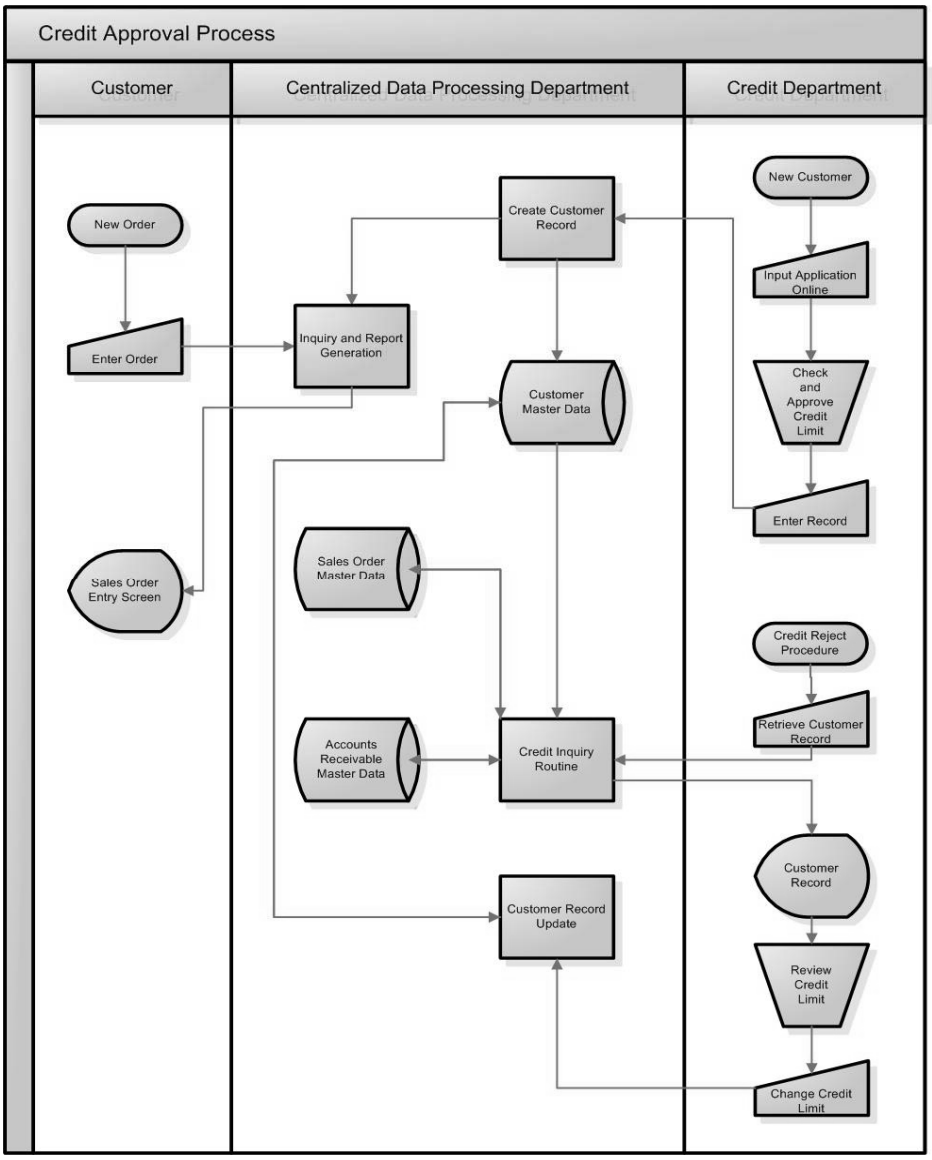
The hacking incident was not disclosed until after the hacker was caught and indicted. When the news of the hacking incident emerged on March 3, 2005 through the jury's indictment, the stock market reacted to the news by adjusting AlphaCo's stock price as shown in Appendix 4.

APPENDIX 1: FINANCIAL STATEMENTS

Selected Consolidated Financial Data (Dollars in 000s, except per share data)

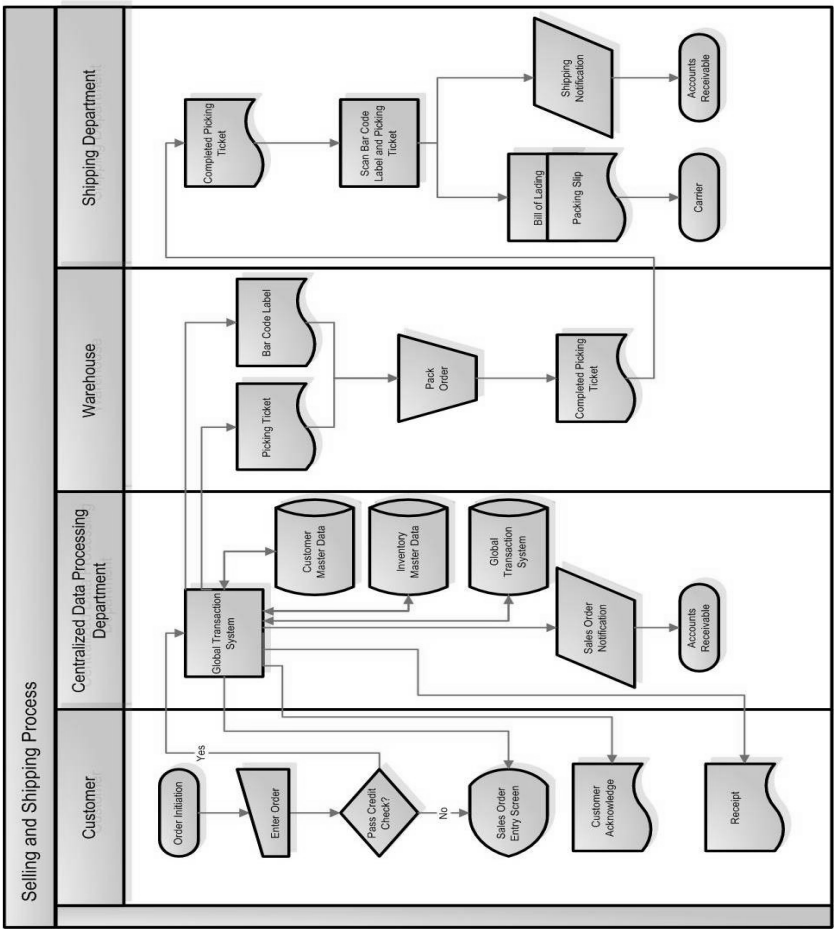
	Fiscal Year				
	2002	2001	2000	1999	1998
Selected Operating Information					
Net sales	$ 42,102,963	$ 33,051,057	$ 24,872,309	$ 18,035,177	$ 12,925,301
Gross profit	$ 2,004,245	$ 2,086,752	$ 1,628,534	$ 1,218,576	$ 908,529
Income from operations	$ 300,006	$ 7,299,078	$ 564,869	$ 371,262	$ 280,322
Income before taxes, minority interest and extraordinary item	$ 435,740	$ 610,290	$ 489,734	$ 295,136	$ 201,924
Income before extraordinary item	$ 269,462	$ 367,763	$ 290,460	$ 166,019	$ 126,461
Net income	$ 275,129	$ 367,763	$ 290,460	$ 166,019	$ 126,461
Basic earnings per share -income before extraordinary item	$ 1.88	$ 2.64	$ 2.15	$ 1.49	$ 1.19
Diluted earnings per share -income before extraordinary item	$ 1.82	$ 2.46	$ 1.98	$ 1.32	$ 1.11
Basic earnings per share -net income	$ 1.92	$ 2.64	$ 2.15	$ 1.49	$ 1.19
Diluted earnings per share -net income	$ 1.86	$ 2.46	$ 1.98	$ 1.32	$ 1.11
Basic weighted average common shared outstanding	$ 215,106,311	$ 208,895,715	$ 203,646,080	$ 168,427,587	$ 160,877,043
Diluted weighted average common shared outstanding	$ 221,677,068	$ 224,306,805	$ 219,461,298	$ 188,154,564	$ 171,776,057
Selected Balance Sheet Information					
Cash	$ 192,228	$ 145,023	$ 138,318	$ 72,419	$ 85,374
Total assets	$ 12,407,891	$ 10,100,106	$ 7,398,227	$ 5,050,421	$ 4,411,347
Total debt	$ 2,022,203	$ 2,580,684	$ 1,711,697	$ 456,050	$ 1,275,822
Stockholders' equity	$ 2,950,268	$ 2,098,886	$ 1,557,309	$ 1,237,725	$ 466,193

APPENDIX 2: CUSTOMER CREDIT APPROVAL PROCESS



Note: This process diagram is created for discussion purposes building on Gelinas, Sutton, and Fedorowicz (2004).

APPENDIX 3: SELLING AND SHIPPING PROCESS

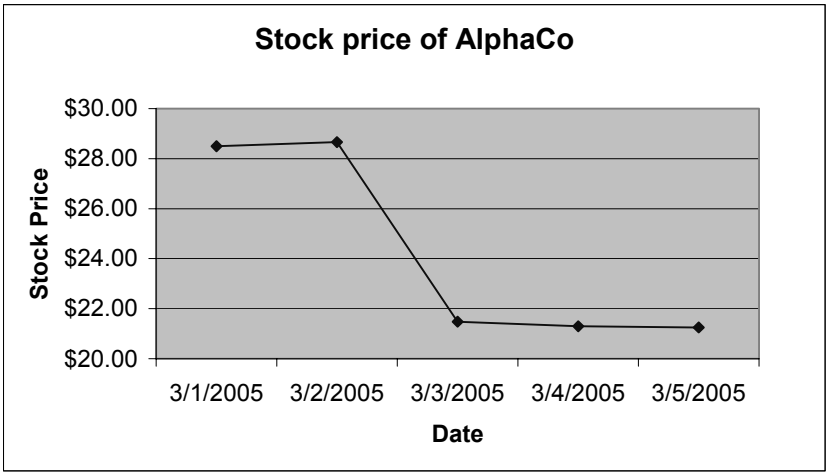


Note: This process diagram is created for discussion purposes building on Gelinas, Sutton, and Fedorowicz (2004).

APPENDIX 4: STOCK PRICE OF ALPHACO AROUND THE ANNOUNCEMENT OF THE HACKING INCIDENT

Date	Open	High	Low	Close	Volume	Adj Close*
1-Mar-05	$28.57	$29.42	$28.44	$28.50	2946200	$28.50
2-Mar-05	$28.50	$29.18	$28.40	$28.66	2855234	$28.66
3-Mar-05	$28.66	$21.90	$21.48	$21.48	3041523	$21.48
4-Mar-05	$21.48	$21.96	$21.00	$21.30	2845294	$21.30
5-Mar-05	$21.30	$21.27	$20.25	$21.25	2975235	$21.25

* Close price adjusted for dividends and splits.



REFERENCES AND ADDITIONAL READINGS

1. AuditNet. (2005). "Fraud/Investigative Resources", http://www.auditnet.org/fraudres.htm, February 9, 2006.
2. AICPA. (2006). "Proposed Statement on Standards for Attestation Engagements, Reporting on an Entity's Internal Control Over Financial Reporting", http://www.aicpa.org/download/exposure/ED_AT_501.pdf, February 25, 2006.
3. COSO. (2006). http://www.coso.org/, February 9, 2006.
4. Fox, C. and Zonneveld, P. (2004). IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting. IT Governance Institute, Rolling Meadows, IL.
5. Gelinas, U.J., Sutton, S.G., and Fedorowicz, J. (2004). Business Processes and Information Technology. Thomson Southwestern Publishing, Mason, Ohio.
6. Hayes Jr., A. (2005). "Fraud Happens. Peering over the Shoulder of an Auditor", http://www.fraudhappens.com/FraudArticle.ivnu, April 18, 2005.
7. Heschl, J. (2005). "Overview of International IT Guidance", COBIT®MAPPING, http://www.isaca.org/Template.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=10016, April 23, 2005.
8. Hunton, J., Bryant, S., and Bagranoff, N. (2004). Core Concepts of Information Technology Auditing. John Wiley & Sons, Hoboken, New Jersey.
9. iLaw Eurasia 2004. (2004, December 14). "Emerging Legal and Policy Issues for the Information Age, Security in the Network Age: Cybercrime and Information Security", http://cyber.law.harvard.edu/ilaw/eurasia_2004_schedule/tuesday, April 8, 2005.
10. ISACA. (2004). "IT Control Objectives for Sarbanes-Oxley: The importance of IT in the design, implementation and sustain ability of internal control over disclosure and financial reporting," http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_7july04.pdf, February 9, 2006.
11. ISACA. (2006). http://www.isaca.org/, February 9, 2006.
12. McInturff, J.T. (2006). "Managing Cyber Risk", http://www.loma.org/res-05-04-cyber-risk.asp, February 9, 2006.

13. Montgomery D., Beasley M., Menelaides S., and Palmrose, Z. (2006). Auditors' New Procedures for Detecting Fraud, http://www.aicpa.org/pubs/jofa/may2002/mont.htm, February 9, 2006.
14. North Carolina Wesleyan College. (2005). "Fraud Audit and Forensic Accounting", http://faculty.ncwc.edu/toconnor/350/350lect05.htm, April 23, 2005.
15. Ramos M. (2006). "Auditors' Responsibility for Fraud Detection-Adapted from Fraud Detection in a GAAS Audit—SAS No. 99 Implementation Guide", http://www.aicpa.org/pubs/jofa/jan2003/ramos.htm, February 9, 2006.
16. Simmons, M. (2005, September 19). "Materiality and Reportable Conditions", http://www.facilitatedcontrols.com/internal-auditing/material.htm, April 18, 2005.

ACKNOWLEDGEMENT

We thank the Austin, Texas Chapter of the Information Systems Audit and Control Association (ISACA), and Steve Sizemore and Ron Franke in particular, for their sponsorship of the Best Student Project Award in the IT Audit & Security Course at the Red McCombs School of Business.

AUTHOR BIOGRAPHIES

Hüseyin Tanriverdi is an assistant professor at The University of Texas at Austin. He teaches IT audit and security and business data communications. He researches risk/return implications of IT and business strategies. His work is published in Strategic Management Journal, MIS Quarterly, Journal of the Association for Information Systems, European Management Journal, Organizational Dynamics, and Telemedicine Journal. Tanriverdi has a Doctorate in Information Systems from Boston University, a M.Sc. in Information Systems from the London School of Economics and Political Science, and M.Sc. and B.Sc. degrees in electrical and electronics engineering from the Middle East Technical University in Ankara, Turkey.

Joshua Bertsch is an Associate in Advisory Services at PricewaterhouseCoopers. His primary focus with the Firm is on Identity Management and IT Effectiveness, performing services for clients around strategic operationalization of enterprise IT systems and security. Mr. Bertsch's professional experiences prior to joining the Firm included key roles within startup, corporate, and academic organizations. He received his Bachelors of Business Administration in MIS and Finance from The University of Texas at Austin McCombs School of Business.

Jonathan Harrison is an associate for KPMG, LLP Information Risk Management Advisory Services. He performs IT Audit and Consulting Services. Mr. Harrison received his Bachelor Degree from The University of

Texas in Austin with a major in Management Information Systems and a minor in Finance. Other professional experience includes Application Development and The System Development Life Cycle.

Po-Ling Hsiao is a Tax Associate at The Walt Disney Company. Mr. Hsiao received his B.A. from Yuan Ze University and Master in Professional Accounting from the University of Texas at Austin. He is CISA Qualified and a Taiwan CPA.

Ketan Mesuria is a Consultant at Ernst & Young in the Legal Technology Services practice. Mr. Mesuria specializes in Computer Forensics, Data Analysis, and Electronic Discovery. Mr. Mesuria recently graduated from the University of Texas at Austin with a Bachelor of Business Administration in Management Information Systems and a minor in Finance.

David Hendrawirawan is a Senior Consultant at Deloitte & Touche Enterprise Risk Services. Mr. Hendrawirawan performs IT Audit and Consulting services. He specializes in ERP Security and Controls, Infrastructure Security, and Database Development. Mr. Hendrawirawan received a Bachelors Degree in Accounting and Masters Degree in Management Information Systems from Texas A&M University.

ALPHACO: A TEACHING CASE ON INFORMATION TECHNOLOGY AUDIT AND SECURITY

TEACHING NOTE

This teaching note is developed as a companion teaching aid for "ALPHACO: A TEACHING CASE ON INFORMATION TECHNOLOGY AUDIT AND SECURITY." The AlphaCo case is designed to foster classroom discussions around IT audit and system security issues, especially in the context of firms that are subject to the Sarbanes-Oxley Act of 2002. The case is most suitable for IT Audit and security courses aiming to teach IT risks, IT controls, and IT audit practices; MIS courses aiming to teach general computer controls and application controls; and accounting courses aiming to teach internal controls and frameworks such as COSO and COBIT.

DISCUSSION POINTS AND GUIDELINES

1. The impact of IT security breaches on firm value

The case can be used to illustrate the impact of IT security breaches on firms. AlphaCo lost about $20 million due to the fraudulent orders placed by the hacker. While this amount may appear small for the $42 billion firm, instructors should draw student's attention to the stock price reactions to the news of the hacking incident. Appendix 4 shows that the stock of AlphaCo lost about 25% of its value within 48 hours of the announcement of the hacking incident. This is a major loss in market capitalization of the firm. Instructors can also discuss damage to the reputation of the firm.

Suggested discussion questions:

- What harm does this hacking incident do to the firm?
- Should the firm disclose the hacking incident to the public? Why?

2. Implications for regulatory compliance

The case can be used to foster a discussion about the importance of IT controls over financial reporting and SOX compliance efforts of firms. With increasing dependence of corporations on information technology, the effectiveness of IT control has an impact on financial reporting as well as the auditor's audit strategy. The COSO framework serves as a plausible tool in evaluating internal controls (See Teaching Note Appendix 1). The COBIT framework integrates internal control with information and information technology (See Teaching Note Appendix 2). These frameworks provide conceptual guidance in designing, implementing, and evaluating internal controls. However, not all

components of these frameworks are related to financial reporting. Auditors take selected controls into account when assessing the effectiveness of IT control over financial reporting.

Section 404 of SOX requires the CEO and CFO to annually state their responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting, conduct and provide an assessment of the effectiveness of the enterprise's internal controls. It also requires the external auditor to attest to the management's assertion and the internal controls identified by the management. Thus, the hacking incident that led to fraudulent orders could have an impact on the firm's financial statement audit.

Section 302 of SOX requires the CEO and CFO of a public company to certify quarterly and annually that they are responsible for disclosure controls, they have designed controls to ensure that material information is known to them, evaluated the effectiveness of controls, presented their conclusions in the filing, and disclosed to the audit committee and auditors significant control deficiencies and acts of fraud. Since the firm's IT systems are critical to initiate, record, process, summarize and report accurate financial and non-financial data, the hacking incident could indicate deficiencies in IT controls of the firm and adversely affect the firm's ability to comply with SOX. The figure in Teaching Note Appendix 3 can be used to discuss why IT is important in the design, implementation, and sustainability of internal control over disclosure and financial reporting.

Suggested discussion questions:

- How and why are IT controls relevant to financial reporting?
- How does the hacking incident influence financial statement audit of the firm?
- How does the hacking incident influence firm's ability to comply with SOX?

3. Usage of the COSO and COBIT frameworks

The case intentionally leaves out details about how exactly the hacking incident happened at AlphaCo. The purpose is to foster in-class discussions around internal control weaknesses (IT and non-IT) that could potentially lead to such IT security breaches. Instructors can cover the COSO and COBIT frameworks in advance of this discussion as conceptual tools in thinking about internal controls (See Teaching Note Appendix 1 and Teaching Note Appendix 2). The discussion can be used to teach students the logic of the COSO and COBIT frameworks and how they can be used in designing and testing effective business and IT controls.

Suggested discussion questions:

- Which internal control weaknesses allowed the hacker to break into IT systems of AlphaCo?
- Which internal control weaknesses should the management try to fix immediately? Why?

4. Differences among preventive, detective, compensating or steering controls

Instructors can use this hacking case as a context for introducing and discussing different types of controls such as preventive, detective, compensating or steering controls. Preventive controls are designed to prevent errors or irregularities such as the hacking incident in this case. Detective controls are for detecting errors or irregularities after they occur. If resource limitations preclude the implementation of more direct controls, compensating controls provide reasonable assurance. Steering controls can be designed to guide actions towards desired objectives.

Suggested discussion questions:

- What types of internal controls allowed the firm to detect the fraud?
- What types of internal controls can the firm design to detect fraud much earlier in the future?
- What types of internal controls can be designed to prevent future occurrences of hacking?

5. External auditor's and management's responsibility for detecting and reporting fraud

The case can be used to foster discussions about external auditor's and management's responsibilities for detecting and reporting fraud. The case states that the audited financial report of AlphaCo in 2002 did not make any reference to the hacking incident, the resulting fraudulent activity, or the loss of approximately $20 million. It could be because the fraud was not classified as a significant deficiency or material weakness. The magnitude of the fraud ($20 million) was probably well below the materiality level for the $42 billion firm; it was detected by AlphaCo's internal control systems; compensating controls were immediately in place; and the likelihood of reoccurrence was remote.

Suggested discussion questions:

- What are managers' responsibilities for detecting and reporting fraud?
- What are external auditors' responsibilities for detecting and reporting fraud?
- Why did the audited financial report of AlphaCo in 2002 not make any

reference to the hacking incident, the resulting fraudulent activity, or the loss of approximately $20 million?

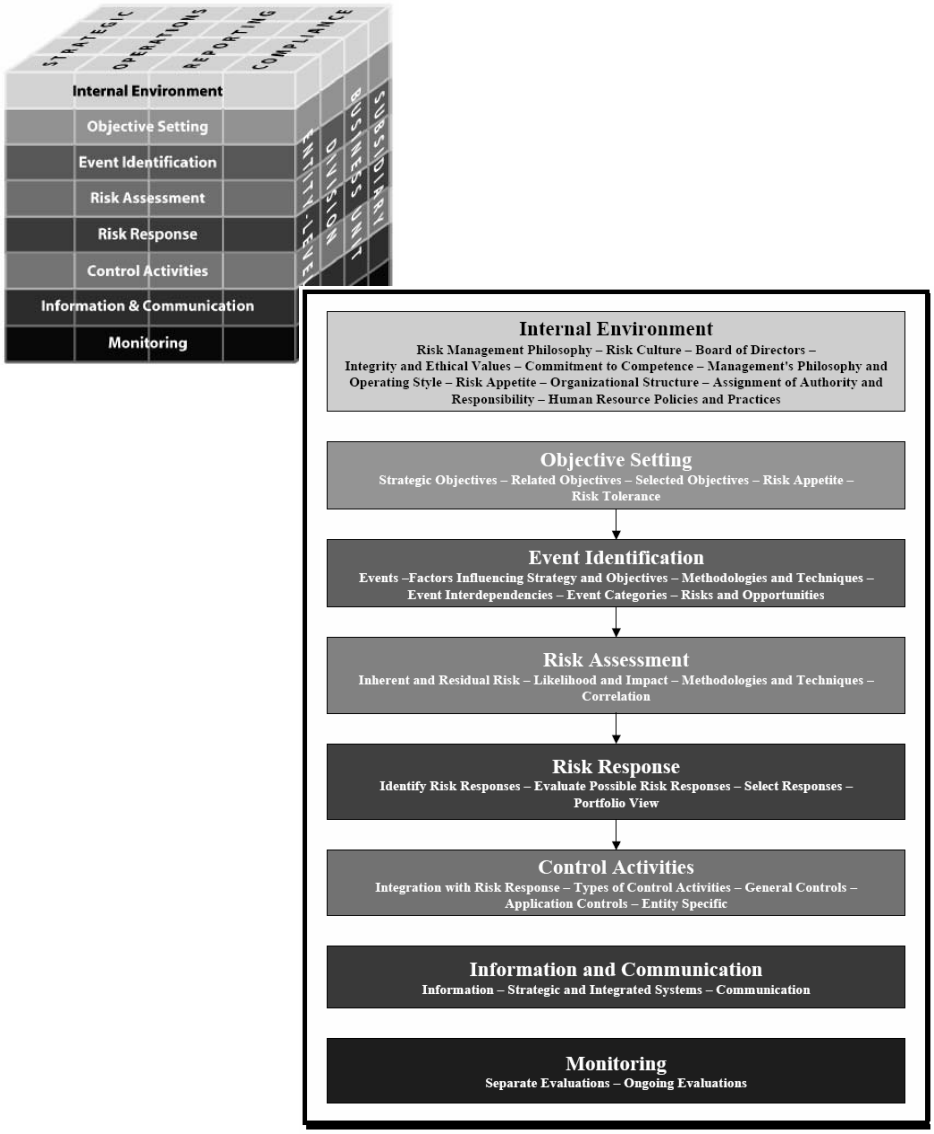
- What criteria do auditors use to classify a control exception into Deficiency, Significant Deficiency, and Material Weakness categories?
- Under what conditions does an IT control exception become classified as a Deficiency, Significant Deficiency, or Material Weakness?

SAS (Statements on Auditing Standards) No.1 states: "The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Because of the nature of audit evidence and the characteristics of fraud, the auditor is able to obtain reasonable, but not absolute, assurance that material misstatements are detected. The auditor has no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by error or fraud, that are not material to the financial statements are detected."

SAS No. 99 describes a process in which the auditor (1) gathers information needed to identify risks of material misstatement due to fraud; (2) assesses these risks after taking into account an evaluation of the entity's programs and controls; and (3) responds to the results. Auditors should comply with AICPA (American Institute of Certified Public Accountants) professional standard to help clients prevent fraud. The risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures.

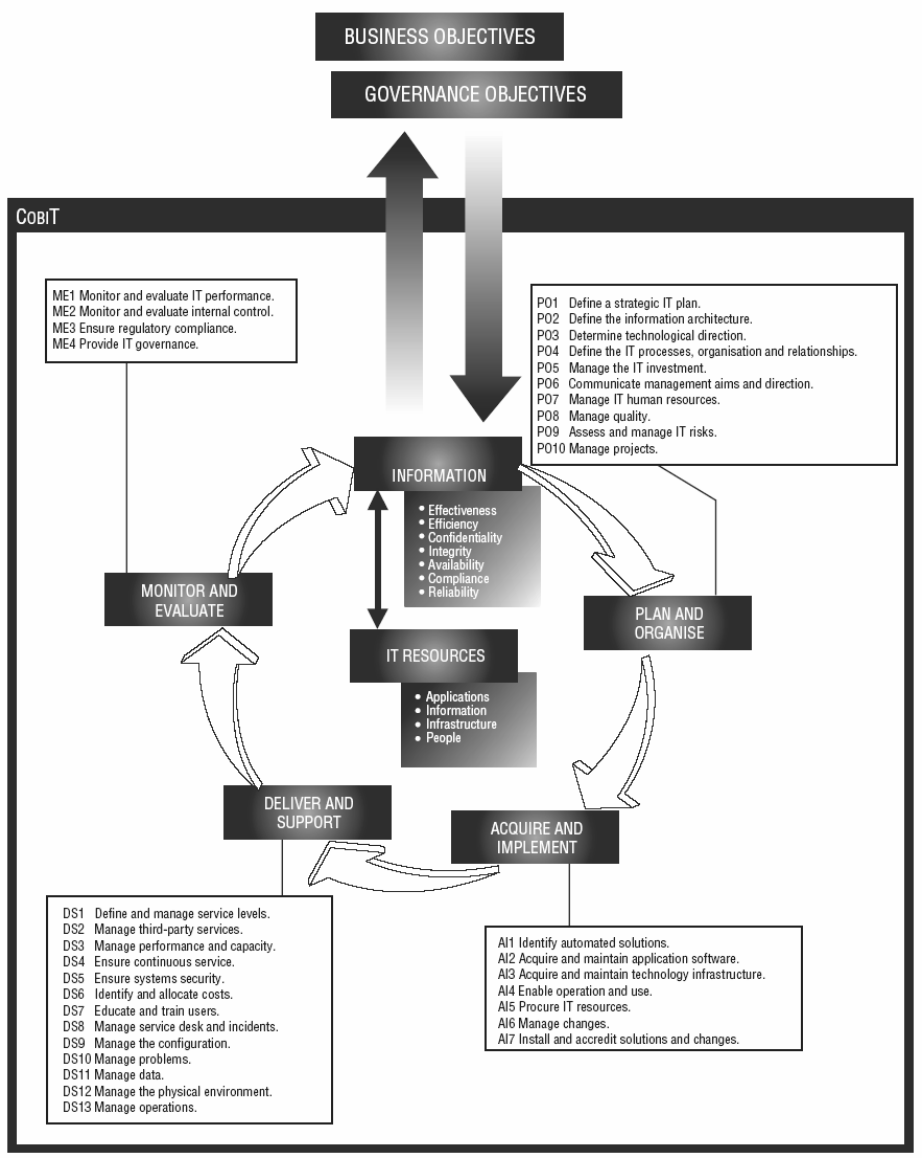
The Sarbanes-Oxley Act created new responsibilities for both the accounting profession and corporations. The main responsibility of detecting fraud still falls on management. Management is now required to assess the company's system of internal control prior to the audit. Then, the auditors attest to the accuracy of the management's assertions on internal control. The auditor is required to thoroughly document testing done in attesting to management's assertions on the effectiveness of their internal control system. To form an opinion as to whether control systems provide managers with reasonable assurance that desired business outcomes will be achieved, the auditor has to consider the issue of materiality. Instructors can refer to AICPA (2006) in our reference list for specific guidance on evaluating control exceptions and deficiencies.

TEACHING NOTE APPENDIX 1: COSO ERM FRAMEWORK AND COMPONENTS



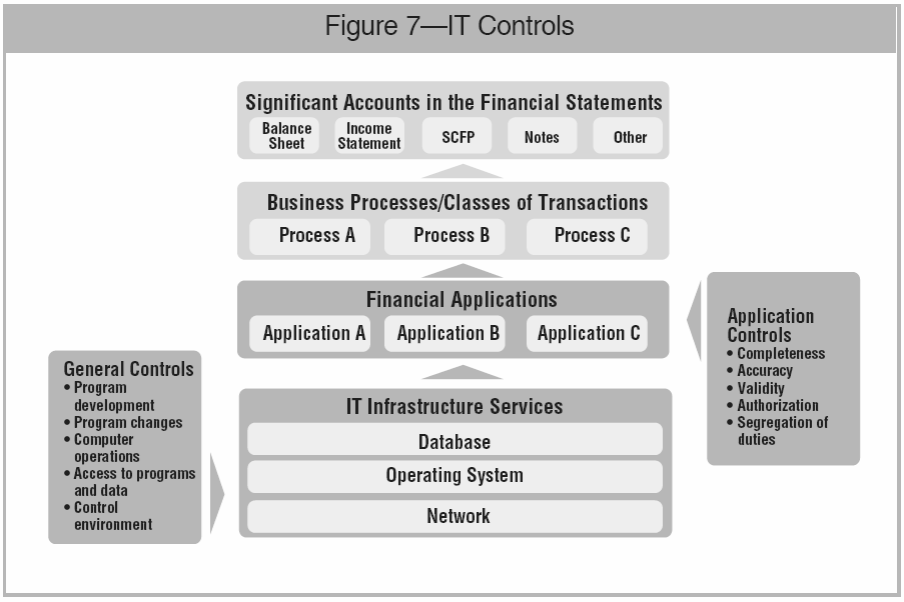
Sources: Enterprise Risk Management—Integrated Framework: Executive Summary and Framework, Exhibit 1.1, p. 23; and Enterprise Risk Management—Integrated Framework: Application Techniques, Exhibit 1.1, p. 2. Copyright © 2004 by the Committee of Sponsoring Organizations of the Treadway Commission. Reproduced with permission from the AICPA acting as authorized copyright administrator for COSO.

TEACHING NOTE APPENDIX 2: COBIT FRAMEWORK



Source: COBIT 4.0, used by permission of the IT Governance Institute (ITGI). 1996, 1998, 2000, 2005 IT Governance Institute (ITGI). All rights reserved. COBIT is a registered trademark of ISACA and the IT Governance Institute.

TEACHING NOTE APPENDIX 3: IT CONTROLS



Source: IT Control Objectives for Sarbanes-Oxley, used by permission of the IT Governance Institute (ITGI). ©2004 IT Governance Institute (ITGI). All rights reserved.