ISSUES IN ACCOUNTING EDUCATION
Vol. 26, No. 3
2011
pp. 521–545

American Accounting Association
DOI: 10.2308/iace-50031

Breach of Data at TJX: An Instructional Case Used to Study COSO and COBIT, with a Focus on Computer Controls, Data Security, and Privacy Legislation

Sandra J. Cereola and Ronald J. Cereola

ABSTRACT: Internal control frameworks (ICF) provide a basis for understanding controls in an organization and for making judgments about the effectiveness of controls. The Sarbanes-Oxley Act of 2002 (SOX) requires companies to report, on an ongoing basis, the effectiveness of their internal controls in their annual filings. The Securities and Exchange Commission (SEC) recommends companies use ICF to help achieve compliance with SOX. ICF provide a useful tool for management and auditors evaluating and addressing the adequacy of controls in their organization. As there is no such thing as a "risk-free" enterprise, developing an understanding of ICF is important for students entering the accounting profession. This instructional case provides students the opportunity to assess internal control risks within an organization's information system using a "real-world" problem following COSO (SEC-recommended ICF) and/or COBIT as a guide. Students then evaluate the organization's overall level of internal control risks and formulate recommendations for mitigating such risks.

Keywords: internal controls; COSO; COBIT; internal control framework; data security.

THE CASE: TJX SECURITY BREACH

You are a recent graduate and have accepted an accounting position with one of the big accounting firms in Massachusetts. Prompted by the discovery of a computer breach of their corporate systems, TJX Companies (hereafter, referred to as TJX) hires your firm to review and assess the internal controls related to their information security program and to advise them as to whether they are in compliance with applicable laws and regulations. As one of your first assignments, you are placed on the TJX task force. This assignment requires you to use your knowledge of internal control frameworks (ICF), including the Committee of Sponsoring Organizations Integrated Framework (COSO) (1992), the Control Objectives for Information and

Sandra J. Cereola is an Assistant Professor and Ronald J. Cereola is an Assistant Professor, both at James Madison University.

Published Online: August 2011

related Technology framework (COBIT), state and federal compliance laws[1] and other applicable federal and state information security laws and regulations,[2] as well as supplemental evidence, which you will be required to discover through research of credible sources and cite in your report, to analyze the case narrative provided on TJX. Upon your review, you are required to prepare a comprehensive written report discussing your evaluation of TJX's internal controls. The report will first be presented to your firm's top management team and then in summary to TJX's management team.

In preparation for your involvement with this task force, you are required to review the internal control framework(s) that you are assigned to use to assess compliance (i.e., COSO and/or COBIT). The focus of your review will be only on those aspects of COSO and/or COBIT that are significant to financial reporting and information security.

Company Background

TJX is one of the largest international off-price apparel and home fashions retailers in the U.S., with over 2,700 stores worldwide at the end of fiscal 2009. Based in Framingham, Massachusetts, the company was founded in 1956 as Zayer's discount department stores. Diversifying into specialty retailing, the company acquired Hit or Miss in 1969 (an off-price fashion clothing chain for women), and opened its first T.J. Maxx store in 1977 (modeled after the Marshalls chain, an off-price fashion store for the whole family). Other TJX ventures in the off-price fashion market included acquisitions of companies such as Chadwicks of Boston, B.J.'s Wholesale Club, and Home Club. In 1987, Zayer went public, organizing as TJX Companies Incorporated (found on the NYSE under the ticker symbol TJX). In 1996, TJX is added to the Standard & Poor's S&P 500, and by 2009 the company is ranked 119th in the Fortune 500.

Since its inception, TJX's operations have remained steadfast. Based on the 2009 annual report, the company operates five business segments (three reside in the U.S., and one each in Canada and Europe), including eight retail chains. Each segment has its own administrative, buying and merchandising, and organization and distribution network. The eight retail chains include T.J. Maxx, Marshalls, Home Goods, A.J. Wright, HomeSense-Canada, StyleSense, T.K. Maxx, and HomeSense-Europe, selling brand name items ranging from family apparel, accessories, bedding, and furniture to jewelry, beauty products, and housewares. TJX's core-target customer includes the middle- to upper middle-income shopper. Consolidated net sales in 2009 were over $20 billion, total assets over $7 billion, and operating cash flows over $2 billion (for financial information, visit TJX Companies website).

Among the key success factors for TJX's rapid growth are its flexible business model and its corporate culture. TJX's culture centers on the management and staff acting with integrity, and emphasizes that all people must be treated with dignity, respect, and caring. They operate under the Remember Everyone Affects Customer Happiness (REACH) philosophy, which is dedicated to providing customers, vendors, and co-workers with a level of caring that goes beyond stakeholder expectations. Further, it is a culture in which success is measured not only on delivering results, but also on how those results are achieved.

Information Technology

The success of TJX depends critically on their operational performance and the information systems upon which their operations are based. Success, therefore, depends on TJX's ability to have

[1] Key laws include the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Children's Online Privacy Protection Act (COPPA).

[2] Other regulations promulgated by the Payment Card Industry (PCI), Federal Trade Commission (FTC), and individual states.

information systems that permit them to maintain a flexible business model, engage in opportunistic purchasing, maintain an efficient inventory management system, and maintain low-cost operations.

As is prevalent in today's businesses, TJX relies heavily on its information systems and, thus, the ability to operate such systems efficiently and effectively has a significant impact on their overall business operations. Implementing effective internal controls that ensure data reliability, security, and confidentiality, along with an adequate disaster recovery plan, is essential for ongoing operations and for reducing litigation risk.

Operations at TJX in 2009 include 19 distribution centers (13 located domestically and six internationally). Information systems are managed through corporate computer networks and in-store networks. The networks are linked worldwide, connect corporate headquarters with each store, and are used for administrative purposes, as well as for processing sales transactions. These networks also provide access for wireless devices used at each store.

In its daily operations, TJX uses computer networks to collect transaction information, including personal information from customers as needed for credit card and debit purchases, personal check verification, and un-receipted returns. Examples of data collected include credit/debit account numbers, expiration dates and electronic security codes for payment authorization, bank routing numbers, account and check numbers, driver's license numbers, date of birth, name, address, and/or other personal identification numbers (military or state documentation). The information collected is used to obtain payment authorization and is transmitted from the in-store networks to designated computers on the central corporate network, and from there to bank networks. In response, the banks send authorization transmissions back to the corporate networks, and this information is then transmitted back to the in-store networks.

The Data Security Breach

On December 18, 2006, TJX discovered an unauthorized intrusion into their computer systems that process and store information related to customer transactions. The intrusion was identified through suspicious software found on TJX's computer systems. Upon discovery, TJX employed both General Dynamics Corporation (GDC) and International Business Machines Corporation (IBM), two leading computer security and incident response companies, to help with the investigation.

The investigation began with an examination of TJX's accounting information systems (AIS), with the purpose of detecting anomalies in the system. On December 21, 2006, GDC and IBM determined that TJX's systems had indeed been breached and that an intruder was still in their AIS. A security plan was set in motion designed to monitor the ongoing intrusion, protect customer data, and strengthen the systems' security from future attacks.

Events following the breach included TJX contacting the appropriate law enforcement authorities, including the U.S. Department of Justice, U.S. Secret Service, and the U.S. Attorney's Office in Boston, Massachusetts, on December 22, 2006. Upon notification, TJX was advised by the U.S. Secret Service not to disclose the breach publicly at this point, as it would impede upon further investigation. On December 26th and 27th, contracting banks and debit, credit, and cash processing companies were notified of the intrusion.

During the ongoing investigation, it was determined that personal, confidential customer information was stolen, and that the scope of the breach spanned approximately 18 months. Public notification of the intrusion was released on January 17, 2007, in a press release issued to the public (for a complete copy of the press release, go to www.tjx.com and click on Investor Information and then Press Releases; all releases are in chronological order). In the release, the Chairman and acting Chief Executive Officer (CEO) stated:

> We are deeply concerned about this event and the difficulties it may cause our customers. Since discovering this crime, we have been working diligently to further protect our customers and strengthen the security of our computer systems, and we believe customers should feel safe shopping in our stores. Our first concern is the potential impact of this crime on our customers, and we strongly recommend that they carefully review their credit card and debit card statements and other account information for unauthorized use. We want to assure our customers that this issue has the highest priority at TJX.

As a result of the breach and as a courtesy to its customers, TJX established a special helpline and created a special link on its company website which provided updated information on the breach.

The investigation determined that the scope of the intrusion spanned from July 2005 until it was detected on December 18, 2006. The breach occurred in computer operations at two corporate offices, one located domestically and one internationally. Both corporate offices process and store information related to payment card, check, and un-receipted merchandise return transactions for its customers. Confidential customer information stored at these locations included debit/credit card information, as well as personal customer information provided with un-receipted returns (these included customer names and addresses, driver's license numbers, and military/state identification numbers, some of which were the same as the customers' social security numbers).

Details of the examination revealed that the intruders' initial point of access occurred in the computer systems located in a Framingham, Massachusetts, store. Using directional antennas and a laptop computer, the perpetrators intercepted electronic transmissions sent over TJX's wireless network. These transmissions included authorization requests, credit and debit card payments, and other personal customer information. TJX's systems, at that time, transmitted wireless transactions using Wired Equivalent Privacy (WEP) technology. Other points of entry occurred at in-store computer kiosks. Each kiosk is equipped with a personal computer (PC)-style system that is directly connected to the corporate network and is used to capture jobseeker information. The intruders connected USB drives with utility programs to these computers and then later used these terminals to access the corporate network.

Electronic footprints left behind by the intruders on the TJX network identified encrypted messages indicating which files had been copied. With these footprints, investigators were able to piece together the dates as to when most of the data was stolen and found that most occurred during peak sales periods. However, because of the technology used by the intruder, it was difficult for TJX to determine the contents of the files that were stolen. Other evidence revealed that the intruders used key logging technology to obtain user identification and password information from the corporate network and then used this information to create fictitious accounts. These accounts were later used to collect transaction information remotely.

Current Events/Financial Impact

Since the data breach, TJX has taken steps to increase computer security and protocols and instituted an ongoing program to monitor data security. From the time of discovery, in 2006, to 2009, TJX expensed $171.5 million pre-tax related to the computer intrusion, and maintains $42.2 million reserve for future losses related to the breach.

TJX press releases highlighting the financial impact indicated: On November 30, 2007, TJX announced an agreement with Visa USA and Visa Inc. to fund up to a maximum of $40.9 million pre-tax in alternative recovery payments. On April 2, 2008, TJX announced agreement with MasterCard International Inc. to fund up to a maximum of $24 million pre-tax in alternative recovery payments. On June 23, 2009, TJX announced a settlement with a multi-state group of 41 Attorneys General relating to the data breach. In the settlement, TJX established a $2.5 million Data

Security Fund for use by states to advance data security and technology, provided $5.5 million to cover states' expenses (including $1.75 million to cover investigation expenses), certified TJX's computer systems meet detailed data security requirements specified by states, and encouraged development of new technologies to address vulnerabilities in payment card systems.

Other Information

Regulatory Complaints: In light of the data breach, the Federal Trade Commission (FTC) filed a complaint against TJX Companies in 2008, indicating that they had violated the provisions of the FTC Act (FTC 2008). The complaint alleged that TJX engaged in a number of practices that failed to provide reasonable security of personal information in its networks and, as such, resulted in a computer intrusion (for a complete copy of the FTC complaint, visit www.ftc.gov, click on Actions, then Cases by Name, and search for "The TJX Companies, Inc."; Docket No. C-072-3055).

Payment Card Industry Standards: All organizations that accept, transmit, or store cardholder information must follow Payment Card Industry Data Security Standards (PCI DSS) (PCI Security Standards Council 2008). TJX utilizes commercially available systems to process payment card and personal information. The technology used for data transmissions and approval is determined and controlled for by the payment card industry (PCI).

CASE REQUIREMENTS AND QUESTIONS

As part of your first assignment on the TJX task force, you will be responsible for one or more of the following case requirements listed below. Before starting the requirements, read the case material. To successfully complete the case, you are required to obtain supplemental evidence obtained through discovery research of credible sources external to the information provided in the case (e.g., TJX website, TJX 10-K reports, etc.).

Assignment 1

1992 COSO Framework Assessment Requirements

Using the 1992 COSO framework, perform a robust risk assessment of the case, identifying any internal control issues related to each of the five 1992 COSO components identified below. Next, classify each internal control issue as a strength or weakness, and then for each weakness, assess its risk as high, moderate, or low (high risk occurs when a company does not have any corrective actions in place when a key internal control weakness is found, and the company suffers a substantial loss as a result; moderate risk occurs when an internal control weaknesses is found and the company does not have any corrective actions in place, however, only minor losses may occur as a result; and a low risk occurs when an internal control weakness is found and is considered a control deficiency). Finally, classify each risk as a financial, compliance, and/or operational risk (financial refers to internal controls designed to provide reasonable assurance regarding the reliability of the financial statements; compliance is concerned with adherence to rules, policies, and procedures, both internal and external to the organization; and operational is concerned with the effectiveness and efficiency of the organization's activities and whether they help to reduce risks faced by the organization). Use Exhibit 1 to document your work.

1. Control Environment: Includes the evaluation of both soft and hard controls. Soft controls consist of integrity and ethical values, commitment to competence, board of directors and audit committee, and management's philosophy and operating style. Hard controls include organizational structure, assignment of authority and responsibility, and human resource policies and procedures.

EXHIBIT 1

Requirement 1
TJX 1992 COSO Risk Assessment Matrix

Risk Assessment (High, Moderate, or Low); Type Risk (F = Financial, C = Compliance, and/or O = Operational)

Note: When completing this requirement, additional rows may be added as needed.

COSO Component	Control Issue	Strength or Weakness	Risk Assessment	Type Risk
1. Control Environment:	TJX does not have a board of directors information technology committee	Weakness	Low	F, C, O
2. Risk Assessment				
3. Control Activities				
4. Information and Communication				

(continued on next page)

EXHIBIT 1 (continued)

COSO Component	Control Issue	Strength or Weakness	Risk Assessment	Type Risk
5. Monitoring				

2. Risk Assessment: Relevant risks that can impact organizational goals and objectives are identified and assessed. Includes risk assessment in relation to company-wide objectives, process-level objectives, risk identification and analysis, and managing change.
3. Control Activities: Include policies and procedures in place that limit risks that may impact organization's objectives. Examples include activities related to security (application and network), application change management, business continuity and backups, and outsourcing.
4. Information and Communication: Relevant information must be identified, captured, and communicated in a form and timeframe that allows individuals to carry out their responsibilities. Assessment involves evaluating the quality of information and effectiveness of the communication.
5. Monitoring: A process must exist to verify internal control systems are functioning over time. Accomplished through ongoing monitoring, separate evaluations, and reporting of deficiencies.

Assignment 2

2004 COSO ERM Framework Assessment Requirements

Using the COSO ERM framework (COSO 2004), perform a robust risk assessment identifying any internal control issues related to each of the eight components identified below. Next, classify each internal control issue as a strength or weakness, and then, for each weakness, assess its risk as high, moderate, or low (high risk occurs when a company does not have any corrective actions in place when a key internal control weakness is found, and the company suffers a substantial loss as a result; moderate risk occurs when an internal control weaknesses is found and the company does not have any corrective actions in place, however, only minor losses may occur as a result; and a low risk occurs when an internal control weakness is found and is considered a control deficiency). Finally, classify each risk as a financial, compliance, and/or operational risk (financial refers to internal controls designed to provide reasonable assurance regarding the reliability of the financial statements; compliance is concerned with adherence to rules, policies, and procedures, both internal and external to the organization; and operational is concerned with the effectiveness and efficiency of the organization's activities and whether they help to reduce risks faced by the organization). Use Exhibit 2 to document your work.

EXHIBIT 2

Requirement 2
TJX 2004 COSO ERM Risk Assessment Matrix

Risk Assessment (High, Moderate, or Low); Type Risk (F = Financial, C = Compliance, and/or O = Operational).

Note: When completing this requirement, additional rows may be added as needed.

COSO ERM Component	Control Issue	Strength or Weakness	Risk Assessment	Type Risk
1. Internal Control Environment	TJX does not have a board of directors information technology committee	Weakness	Low	F, C, O
2. Objective Setting				
3. Event Identification				
4. Risk Assessment				
5. Risk Response				

(continued on next page)

EXHIBIT 2 (continued)

COSO ERM Component	Control Issue	Strength or Weakness	Risk Assessment	Type Risk
6. Control Activities				
7. Information and Communication				
8. Monitoring				

1. Internal Environment: Encompasses the tone of the organization, sets the basis for how risk is perceived and addressed.
2. Objective Setting: Ensures management has in place a process to set objectives that support and are in line with the entity's mission and are consistent with their risk appetite.
3. Event Identification: Identifies internal and external events that may impact the achievement of an entity's objectives, distinguishing between risks and opportunities.
4. Risk Assessment: Analyzes risks, considering the likelihood and impact as a basis for how risks should be managed.
5. Risk Response: Management selects a risk response: avoiding, accepting, reducing, or sharing risk; develops a set of actions aligned with the entity's risk tolerance and appetite.
6. Control Activities: Include policies and procedures in place that limit risks that may impact the organization's objectives. Examples include activities related to security (application and network), application change management, business continuity and backups, and outsourcing.
7. Information and Communication: Relevant information must be identified, captured, and communicated in a form and timeframe that allows individuals to carry out their responsibilities. Assessment involves evaluating the quality of information and effectiveness of the communication.

EXHIBIT 3

Requirement 3
TJX 2007 COBIT Risk Assessment Matrix

Risk Assessment (High, Moderate, or Low); Type Risk (F = Financial, C= Compliance, and/or O = Operational)

Note: When completing this requirement, additional rows may be added as needed.

COBIT Component	Control Issue	Strength or Weakness	Risk Assessment	Type Risk
1. Plan and Organize (IT environment)	Assessment of Risks—lack of control over information technology environment	Weakness	High	F, C, O
2. Acquire and Implement (program development and change)				
3. Deliver and Support (computer operations and access to programs and data)				

(continued on next page)

EXHIBIT 3 (continued)

COBIT Component	Control Issue	Strength or Weakness	Risk Assessment	Type Risk
4. Monitor and Evaluate (IT environment)				

8. Monitoring: A process must exist to verify internal control systems are functioning over time. Accomplished through ongoing monitoring, separate evaluations, and reporting of deficiencies.

Assignment 3

2007 COBIT Framework Assessment Requirements

Using the 2007 COBIT framework related to each of the four domains identified below, perform a robust risk assessment identifying any internal control issues related to the use of information technology. Next, classify each internal control issue as a strength or weakness, and then, for each weakness, assess its risk as high, moderate, or low (high risk occurs when a company does not have any corrective actions in place when a key internal control weakness is found, and the company suffers a substantial loss as a result; moderate risk occurs when an internal control weakness is found and the company does not have any corrective actions in place, however, only minor losses may occur as a result; and a low risk occurs when an internal control weakness is found and is considered a control deficiency). Finally, classify each risk as either a financial, compliance, and/or operational risk (financial refers to internal controls designed to provide reasonable assurance regarding the reliability of the financial statements; compliance is concerned with adherence to rules, policies, and procedures, both internal and external to the organization; and operational is concerned with the effectiveness and efficiency of the organization's activities and whether they help to reduce risks faced by the organization). Use Exhibit 3 to document your work.

1. Plan and Organize: Define strategic plan, identify IT that may contribute to the achievement of business strategy/objectives, ensure compliance with external requirements, assess risk, and manage projects.
2. Acquire and Implement: Acquire, develop, and implement IT solutions identified.
3. Deliver and Support: Concerned with the delivery of required services, including support, training, education, security, and continuity. Manage configuration, data, facilities operations, and problems.
4. Monitor and Evaluate: Assess IT for quality and compliance (management oversight, independent assurance by internal and external sources, independent audit).

EXHIBIT 4

Requirement 4
1992 COSO-2007 COBIT Mapping Matrix

Note: When completing this requirement, additional rows may be added as needed.

	COSO Component				
COBIT Component	**Control Environment**	**Risk Assessment**	**Control Activities**	**Information & Communication**	**Monitoring**
Plan and Organize		COBIT 1 Assessment of Risks: lack of control over information technology environment			
Acquire and Implement					

(continued on next page)

EXHIBIT 4 (continued)

COBIT Component	COSO Component Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Deliver and Support					
Monitor and Evaluate					

Assignment 4

COSO-COBIT Mapping Requirement

COSO and COBIT cater to different audiences. Whereas COSO's target audience is management at large, COBIT's target audience is management, users, and auditors. Because of these differences, auditors should not expect a one-to-one relationship between COSO's components and COBIT's domains. The purpose of mapping is to give auditors a point of reference when discussing the role of technology in the assessment of internal controls for financial reporting.

Based on your solutions for the 1992 COSO Framework and 2007 COBIT framework requirements, map your internal control issues identified in the four COBIT domains with the five 1992 COSO components. Use Exhibit 4 to document your work. (Note: there are many publications that can help you with the mapping task. For example, the IT Governance Institute [ITGI] provides a publication that maps COBIT to COSO and can be found on the ISACA website: *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Controls over Financial Reporting, Second Edition* [ITGI 2006].)

EXHIBIT 5

Requirement 5
Report Guidance

Report Name:
TJX Companies:
Student's Name:
Date:

Background: Write a short description of TJX Companies and the data security breach.

Purpose: Briefly describe the purpose of the internal control review and why it is important.

Scope: Provide an outline of the scope of the review and a short description of the work that your team performed for TJX Companies.

Findings: Elaborate on the team's key finding(s). Provide specific examples of control strengths and weaknesses. Provide enough detail to support your assessment, particularly for those areas that you feel are high risk and that may impact compliance. For each control given a risk rating of "high," suggest a resolution that will help the company to comply with any applicable regulations. Note that your arguments must be consistent with your assessment.

Conclusion: Provide a statement of your overall assessment of controls at TJX. For example, "Based on our findings, our task force finds TJX is/is not in compliance with SOX for the following reasons. In addition, we find that TJX is/is not in compliance with _______________ (identify other regulatory requirements that you may have encountered during your research of TJX, such as PCI DSS) for the following reasons."

Note: Keep in mind as you write your report that senior executives and managers are very busy and will not spend time reading a report that is of little interest to them. Therefore, limit your report to no more than five pages. If your title and opening paragraphs do not capture their interest quickly, they will likely discard it and move on to the next task. With this in mind, create a catchy title for your report and prepare a compelling introduction that will intrigue the executives, capture their attention, and entice them to continue reading.

Assignment 5

Written Internal Control Assessment

Prepare a written report evaluating the internal controls at TJX. Provide specific examples of control strengths and weaknesses, and identify areas that you feel are *not* in compliance with SOX and other regulatory requirements (use the exhibits above to support your assessment). Written assessment should not exceed five pages. Exhibit 5 is provided as report guidance.

CASE LEARNING OBJECTIVES AND IMPLEMENTATION GUIDANCE

Introduction

The Sarbanes-Oxley Act of 2002 (SOX) (U.S. House of Representatives 2002) was established to restore investor confidence in public markets, and has since had a significant impact on firms' internal control policies and procedures. Section 404 of the Act requires firms to report, on an ongoing basis, the effectiveness of their internal controls in their annual 10-K filings. The reporting requirements include disclosing information about the viability of these controls and any potential risks that may impact the company's overall financial position. The Security and Exchange Commission (SEC) recommends the use of internal control frameworks (ICF) to help firms achieve SOX compliance (SEC 2003).

Many companies have turned to the 1992 Committee of Sponsoring Organizations-Internal Control Integrated Framework (COSO 1992) or the 2004 COSO Enterprise Risk Management Framework (ERM)[3] (COSO 2004) for establishing internal controls over financial reporting. The primary objective of COSO is fiduciary, in that it provides a general framework focusing on control objectives for financial and operational processes that impact financial reporting. IT systems are collectively linked to the financial reporting process and must be evaluated, part and parcel, with SOX compliance. COSO does not provide detailed guidance for firms needing to design and implement specific information technology (IT) controls for their organization. To address this exclusion, the IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA) developed the 2007 Control Objectives for Information and related Technology (COBIT) framework as guidance for controls related to IT (ISACA 2007). It is important to note that SOX compliance does not guarantee a "risk-free" enterprise; however, firms can benefit from the use of ICF as a means to establish strong internal controls that reduce risk exposure.

Information technology is highly vulnerable to security threats. Potential security weaknesses, inherent in information and communication technology, create not only technical problems for IT, but also internal control problems for management. It is management's responsibility to develop and implement sound controls that reduce security risks, increase system availability, protect sensitive information, and lower audit costs. Management has a duty to preserve and protect the firm's critical assets; not only the physical assets, but also the "electronic" assets of the firm. If not properly maintained or safeguarded, an information breach can cause significant damage to an enterprise in terms of regulatory risk (laws and regulations governing the collection, use, retention, security, and destruction of data), market risk (breach resulting in insider trading, stock manipulation, or antitrust violations), and business continuity risk (loss of customer confidence, reputation, stock market valuation, or disruption in operations).

With increased regulations addressing internal controls from both within the industry and through legislation, firms are now faced with the challenge of developing internal control programs that are directed at safeguarding sensitive proprietary information (both financial and nonfinancial), as well as private personal information. Compliance with COSO and COBIT can help organizations meet not only the requirements of SOX, but also contribute toward compliance with other regulatory mandates such as data privacy and security laws.

According to the 2008 Identify Theft Resource Center (ITRC) report, information security breaches have increased by 47 percent during the period 2007 to 2008 (ITRC 2008). The American Institute of Certified Public Accountants (AICPA) indicates that information security management,

[3] The 1992 COSO Framework was updated in 2004 to emphasize the importance of identifying and managing risks across the enterprise.

privacy management, and secure data file storage, transmission, and exchange were among the top ten technology initiatives for 2009 (AICPA 2009). Two highly publicized examples of information breaches resulting from internal control weaknesses occurred at both TJX Companies and Hannaford Supermarkets. These highly publicized cases thrust the problem of information security to the forefront of the issues confronting accounting professionals. As a result of the proliferation in information breaches, states across the nation have adopted legislative measures to address the matter, and U.S. companies are now faced with increased regulatory pressure to adopt internal control procedures that effectively protect sensitive, private, and proprietary information retained by their organizations.

In addition to federal and state mandates impacting information security management, such as SOX, industry associations have also promulgated voluntary guidelines, standards, and practices for their respective members. The enactment of complex information security laws has added to this challenge, requiring firms to implement internal control measures that are designed to prevent information breaches. Many states have enacted notice of security breach laws that address what actions must be taken by firms in the event of an information breach. Perhaps the most far reaching of these legislative efforts is the action taken by the Commonwealth of Massachusetts. Massachusetts (as a result of the TJX breach) enacted a data privacy and security law, 201 CMR 17.00, that emphasizes preventive, detective, and corrective measures (Commonwealth of Massachusetts 2008). The law imposes on firms a statutory duty to implement measures that ensure the security, integrity, and confidentiality of all personal information retained by the organization. The law mandates specific minimum standards that must be met by firms relative to safeguarding personal information obtained in either paper or electronic form. The law requires firms[4] (regardless of size) to formulate a complex comprehensive written security plan that encompasses administrative, technical, and physical safeguards for all personal information obtained.[5]

The instructional case is developed based on current events related to information breaches, and illustrates the consequences of poor internal controls related to information systems and data security. The material provides students an opportunity to learn about the importance of developing, implementing, and monitoring internal control programs that are designed to protect sensitive information from being purloined. This includes not only internal controls designed to improve financial reporting as regulated by state and federal laws, but also programs aimed at the protection of all sensitive information, such as protecting confidential proprietary information from competitors. The case allows faculty to integrate the use of internal control frameworks, such as COSO and COBIT, to teach students how to identify internal control weaknesses, both internal and external, to an organization. It also permits faculty to provide students with hands-on experience assessing risk as it relates to organizations' use of information technology.

Overview and Learning Objectives

In recent years, accountants, auditors, and managers alike have increased their focus on internal controls as a direct result of financial regulations such as SOX and other information security laws. In addition, increased use of complex information technology has changed the way firms gather and report information, further complicating assessment of compliance with these laws and regulations. Several internal control frameworks have been developed that assist firms in establishing compliance, such as the COSO and COBIT, as well as auditing standards such as SAS 109[6]

[4] The provisions of the Massachusetts law apply to all persons that own, license, store, or maintain personal information about residents of the Commonwealth of Massachusetts.

[5] See: http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf (ITRC 2008).

[6] SAS 109, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, effective 12/15/2006. A critical component of the standard includes a client's IT system (AICPA 2006).

(supersedes SAS 94). It is important for students entering the accounting profession to obtain an understanding of these frameworks and standards in order to be able to evaluate the internal controls of an organization and to assert whether firms are in compliance.

This instructional case provides students with the opportunity to gain a better understanding of the importance of internal controls and the frameworks which are used to assess compliance. The case is based on the TJX data security breach which occurred between 2005 and 2006. The case provides detailed narrative and supplemental readings of the events that led up to the breach. The students are asked to evaluate this narrative and to research the case from multiple sources in order to develop a risk assessment profile based on information gathered. Students are challenged to think "outside of the box," as at first glance students may not see the link between the weaknesses in the case and its relation to financial reporting risk. Students must use critical thinking skills in order to draw connections between the risks presented in the case and their impact on financial reporting. Students are required to use internal control frameworks, such as COSO and COBIT, to help them organize their evaluation in a logical and thoughtful manner.

The case offers a number of important benefits with respect to auditor evaluation of internal controls. First, it provides students with an opportunity to demonstrate their knowledge of internal control frameworks as it relates to risk assessment. Second, it allows students to see how COSO and COBIT together can help ease the burden of achieving compliance. Third, it provides students an opportunity to see how internal control frameworks can be used for compliance with other regulatory requirements other than SOX, such as Payment Card Industry Data Security Standards (PCI DSS 2008). Finally, it provides students with the opportunity to develop critical thinking skills and professional writing skills.

Case Adaptability

The instructional case as written provides faculty with an opportunity to assign one or all of the requirements presented at the end of the case, depending on the specific objectives covered in their course. Instructors have the opportunity to use this case material to (1) familiarize students with internal control frameworks recommended by the SEC for compliance with SOX, (2) provide students with an opportunity to review and evaluate internal control weaknesses using recommend frameworks, and formulate recommendations that can help thwart such weaknesses through examination of problems encountered in a real-world case, (3) demonstrate how two widely used internal control frameworks, COSO and COBIT, are inextricably linked, as financial reporting processes are driven by information technology systems, and/or (4) demonstrate how internal control frameworks can contribute to compliance with other regulatory requirements beyond SOX, such as information security laws. The case requires students to think about the many challenges that face accounting professionals and management as they attempt to assess overall risk as it relates to internal controls, information technology, and financial reporting.

These learning objectives respond to the need by the profession for accounting students to have specific competencies and skills in areas such as decision modeling, risk analysis, communication via reporting, research, and technology (Foster and Bolt-Lee 2002).

Implementation Guidance

The case is appropriate for undergraduate and graduate accounting information systems (AIS) and auditing courses. At the undergraduate level, our experience indicates that the case should be presented after the concept of internal controls is discussed in class. Discussion of internal controls is covered over two to three 75-minute class periods (introduction to internal control systems and internal control frameworks, computer controls for AIS, and auditing computerized AIS). During the class period where internal control frameworks are introduced, we spend 20–30 minutes discussing the COSO framework, explaining how each of the five components relates to internal controls. At the undergraduate level, we require students to complete only the COSO requirement (instructors can choose to use either the 1992 or 2004 COSO framework, depending on course coverage), and students are given a week to complete the assignment. At this level, we omit the COBIT internal control framework mapping and writing requirements.

Introduction of the case begins with a brief PowerPoint presentation highlighting the five COSO components. Next, a short video is shown describing the TJX data breach. The video was produced by *60 Minutes* and shown on CBS[7] (CBS 2007). This 13-minute video demonstrates how poor internal controls and lack of compliance with laws and regulations can have a large, negative impact on a firm, both in financial and nonfinancial terms. The video is instrumental in getting students engaged in the conversation on internal controls, as many have shopped at TJX stores (e.g., T.J. Maxx, Marshalls, Home Goods, etc.). After watching the video, students are presented with thought questions (thought questions can be found in the supplemental teaching notes) that are designed to help them think about the case from an internal control perspective in order to better analyze and evaluate the case material.

At the graduate level, we spend a considerable amount of time studying both the COSO and COBIT frameworks prior to introduction of the case. We find that introducing COBIT at this level is appropriate, as we explain to students that (1) SOX requires firms to implement an internal control framework used to assess controls within the firm, and recommends the use of COSO,[8] (2) SOX 404 requires firm executives to include an assessment report on the effectiveness of internal controls over financial reporting, *including IT controls*; however, SOX does not provide specific guidance on how to assess controls related to IT, and (3) in light of this omission, COBIT developed by ITGI and ISACA has increasingly become the most widely used framework for assessing IT controls (Ridley et al. 2004; Damianides 2004).

Although most AIS and auditing textbooks contain a thorough introduction of the COSO framework, the same cannot be said for COBIT. Therefore, we provide students with supplemental readings on the topic of COBIT (a list of these readings can be found in the supplemental teaching notes). For example, sample readings include Chapter 3, "Managing IT Risk," from *IT Governance Using COBIT® and Val IT™: Student Book, Second Edition*. This document was published by the IT Governance Institute in 2007.[9] This chapter defines the relevant IT activities (including both general and application controls) from the four COBIT domains (plan and organize, acquire and implement, deliver and support, and monitor and evaluate). Students do not need any practical business experience to understand the ITGI student handbook, as it is written at a level appropriate for undergraduate or graduate students.

In order to help students develop an understanding of the COBIT/COSO mapping requirement, students are provided with additional readings from the *IT Control Objectives for Sarbanes-Oxley* publication. This publication is available from the IT Governance Institute.[10] Appendix B of this document illustrates the IT processes of COBIT and their relationship to the COSO components.

[7] *60 Minutes*, by CBS, investigates the TJX data breach. The video can be found at: http://www.youtube.com/watch?v=MxG2J3bf1BQ

[8] Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 states that management is required to "base its assessment on a suitable, recognized control framework," and identifies COSO as a suitable framework. SAS 109 states that auditors must obtain an understanding of the five COSO components of internal controls.

[9] Instructors can acquire the *IT Governance Using COBIT and Val IT™: Student Book* from the ISACA academic website: http://www.isaca.org/Knowledge-Center/Academia/Pages/IT-Governance-Using-COBIT-and-Val-IT.aspx

[10] Copies of this publication can be found at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Sarbanes-Oxley-2nd-Edition.aspx (ITGI 2006).

Students are also encouraged to use external resources to find other documents containing mappings of COBIT to COSO (additional resources on this topic are provided in the supplemental teaching notes).

At the graduate level, the case is assigned as a group project after the third week of classes. It is our belief that working in a group at the graduate level is more indicative of a real-life work setting and, therefore, appropriate for this assignment. Students are assigned the COSO, COBIT, mapping, and written internal control assessment requirements. Two weeks after the case is assigned, students are required to make a five- to ten-minute presentation in class demonstrating their progress in completing the assignment. (The purpose of this presentation is to encourage students not to procrastinate. The presentations are not graded; we have found that although no grade is assigned to this benchmark, groups tend to do quite well, as presentations in front of their peers make them competitive.) The final project is due at the end of the semester. Note, as an alternative, the case can be adapted by eliminating the COSO requirement (we have found that it is not necessary for students at the graduate level to complete the COSO requirement prior to completing the mapping requirement, as these students generally had a good working knowledge of COSO coming into the course).

Note, at either the undergraduate or graduate level, the case can be completed individually, in teams, or a combination of both. A team project may be more appropriate, as it more closely imitates that which occurs in the business world. In a business setting, teams consist of individuals with diverse skills and personalities. When students are able to develop critical team-building skills, they become more effective managers and leaders. In addition, a team project allows students to develop communication skills, collaboration skills, and conflict resolution skills. We recommend individual projects at the undergraduate level and group projects at the graduate level.

Prerequisite Knowledge

To complete the case in an undergraduate AIS class, students should have a basic knowledge of the following professional and regulatory guidance:

- 1992 Committee of Sponsoring Organizations Report, *Internal Control-Integrated Framework*
- 2004 Committee of Sponsoring Organizations Report, *Enterprise Risk Management Framework*
- 2002 Sarbanes-Oxley Act, Sections 302 and 404

To complete this case in an auditing or graduate AIS class, students should also be familiar with:

- 2007 IT Governance Institute and Information Systems Audit and Control Association, *Control Objectives for Information and Related Technology Framework*
- Statement on Auditing Standards 109, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*
- Public Company Accounting Oversight Board Auditing Standard No. 5, *An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements* (PCAOB 2007) (supersedes PCAOB Auditing Standard No. 2)

Other optional uses for the case may require familiarity with other regulatory guidance, including:

- Federal/State Data Security Laws (refer to Massachusetts law 201 CMR 17.00)
- Payment Card Industry Data Security Standards (PCI DSS)

Additional implementation guidance is provided in the supplemental teaching notes. Included in these notes are sample solutions, suggestions for further adaptations of the case, additional supplemental readings and links to relevant external publications, and sources, discussion notes, and a grading rubric.

Grading the Case

As noted above, instructors may use the case at either the undergraduate or graduate level. At the undergraduate level, the case represented 10 percent of the student's overall grade. At the graduate level, the case represented 20 percent of the student's overall grade. It is estimated that the case will take 20–30 minutes to grade. To help facilitate grading, a grading rubric is included (see the supplemental teaching notes).

Efficacy of the Case

This case has been presented to students at both the graduate and undergraduate levels at an AACSB accounting-accredited university located in the eastern United States. Students were asked to complete a four-question questionnaire prior to completing the case. As most accounting courses provide some coverage of internal controls, the intent of the first four questions was to establish students' baseline knowledge of internal controls. Students were then asked to complete a 14-question questionnaire after completing the case; the first four questions were intended to establish whether the case increased their working knowledge of internal controls. Table 1 provides the results of the questionnaires.

Eighty-three respondents completed the survey, of which 45 were undergraduate students and 38 were graduate students. Based on the pre-questionnaire, on average, respondents indicated that they had taken two accounting courses that covered internal controls and one accounting course that included material on COSO and COBIT. A limitation in this survey is that students were not asked which accounting courses they had taken that covered internal controls. Survey questions were based on a scale of 0–100 (0 = no knowledge, to 100 = advanced knowledge). Responses to working knowledge of internal controls averaged 65.1, working knowledge of COSO averaged 53.5, and working knowledge of COBIT averaged 47.3. Responses to whether students believed that internal controls were important to their professional development averaged 91.5.

Results indicated that students' working knowledge of internal controls pre-case averaged 65.1; post-case averaged 79.2. Although the results show a 14.1 percent increase in working knowledge pre/post case completion, the small increase is not surprising as, based on the university's curriculum, many of the students were either in or had already taken an audit course, including significant coverage of internal controls. The second two questions showed a more significant pre/post impact. When asked if the case increased their working knowledge of COSO/COBIT, initial responses were 53.5 (47.3); post responses averaged 78.0 (75.9). These results indicate that the case was effective in increasing students' knowledge of both internal control frameworks. Not surprisingly, when students were asked if they thought internal controls were important to their professional development, the overwhelming majority strongly agreed (pre 91.5; post 92.6). Overall results of the remaining ten questions, which attempted to establish relevance for the case, were also favorable, with mean scores ranging from 76.3 to 86.6. The highest mean scores came from statements relating to students' interest in the case, real-world applicability, and relevance in identifying internal control weaknesses.

In addition to the survey, students were asked to provide comments on the case. Overall, students indicated that the case provided them with a unique opportunity to develop skills related to risk assessment through identifying internal control weaknesses using recommended internal control frameworks. Students reported that the case forced them to use critical thinking skills in

TABLE 1

Summary of Student Survey Responses (n = 83: 45 Undergraduate; 38 Graduate)

Panel A: Pre-Questionnaire

Statement	**Response (Std. Dev.)**
1. My current working knowledge of internal controls is	65.1 (10.7)
2. My current working knowledge of COSO is	53.5 (13.5)
3. My current working knowledge of COBIT is	47.3 (16.4)
4. Internal controls important to my professional development	91.5 (12.9)

Response Scale (0–100), where 0 = no knowledge, 50 = some knowledge, 100 = advanced knowledge.

Panel B: Post-Questionnaire

Statement	**Response (Std. Dev.)**
1. Case increased my working knowledge of internal controls	79.2 (11.2)
2. Case increased my working knowledge of COSO	78.0 (14.3)
3. Case increased my working knowledge of COBIT	75.9 (21.4)
4. Internal controls important to my professional development	92.6 (18.3)
5. Case relevant in identifying internal control weaknesses	82.6 (16.2)
6. Case helped me understand importance of SOX	76.3 (16.5)
7. Case relevant in identifying specific controls to protect firm resources	81.4 (13.9)
8. Case relevant in identifying specific controls to achieve effective/efficient operations	79.0 (14.6)
9. Case relevant in identifying specific controls to achieve reliability in financial statements	78.7 (13.5)
10. Case relevant in identifying specific controls to achieve compliance with applicable laws	82.3 (13.3)
11. Found case interesting	81.9 (12.5)
12. Case relevant because it was based on a real-world company	86.6 (11.8)
13. Case was understandable, even though I had no formal training in internal control frameworks	82.4 (14.5)
14. Case provided beneficial learning experience	85.2 (11.5)

Response Scale (0–100), where 0 = strongly disagree, 50 = neither agree nor disagree, 100 = strongly agree.

order to develop a link between the case and internal control issues related to financial reporting, and found that the matrices provided much-needed guidance for their analysis. Students suggested that the case helped them to develop a better understanding of the multitude of compliance laws and regulations imposed upon firms, such as SOX and PCI DSS. Other comments suggested that more time be spent in class covering COSO and COBIT, introduce the case earlier in the semester, increase the length of the written assessment, and provide suggestions for outside resources. Overall, students liked that the case had real-world application (see sample student comments in Table 2). On average, the students reported that it took them between eight and ten hours to complete the case.

TABLE 2

Sample Student Comments

Comments
"I liked that the case had real-world application."
"The case was well written and organized. Instructions were clear; however, we were not smothered by 'this is how we have to do it.'"
"I thought the case was a good learning tool and that it helped me to understand the relationship between SOX and the internal control frameworks."
"Overall, I thought the TJX case was interesting and a great educational experience. I've enjoyed telling one of my mentors about it."
"I thought the TJX case was a good learning tool that helped me understand internal controls as it relates to information technology."
"I thought the TJX project was the most interesting and beneficial to my educational experience. The only thing I would change would be the length of the written assessment. We really struggled to not go over the five page limit, and as a result, had to leave out some of our recommendations. I'd recommend you limit this to ten pages."
"I liked the real-world application of the internal controls and being able to read about the internal control issues that I've learned about in AIS and auditing."
"I liked how the case tied in COSO with SOX and other applicable laws."
"I thought the teamwork environment was also an advantage, because it gives us a bit more practice in team management skills."
"I thought the case was an appropriate length, and wasn't too bogged down with minute details."
"Overall, I really enjoyed the project and thought it did a nice job bringing COSO, SOX, COBIT, and the internal control structure lessons together."
"I thought the case was a good example because most if not all of us knew about the TJX information leak and found it fairly interesting."
"I thought the case did a great job in having us explore COSO and COBIT frameworks. It really parallels the real world as I did IT attestation this summer and a lot of the issues came up in the case that apply directly to the real world, logical access, change management, and firewalls and security controls. I knew that these controls were important but I never really understood where they came from, but it seems like they are heavily based in COBIT and COSO and I thought the correlation was great. Overall great project to give."
"One of the things I did find a little frustrating was the amount of assumptions that we had to make about TJX's internal control system. If possible maybe supplying a list of internal control procedures (even if you had to make them up) that TJX had before the breach."
"I liked the TJX case since we had talked about it previously in other classes so it was familiar. The COSO and COBIT parts were interesting but I wish we had spent more time discussing them in class. Maybe if the paper was due the week before the end of class, the last class could be spent discussing what each group discovered in their research. I think that would be an interesting way to cover the material and learn from other groups."

SUMMARY OF TEACHING NOTES

The teaching notes for this case include the following:

1. A suggested solution for the COSO, COBIT, and Mapping Matrix.
2. A suggested solution for the written report.
3. Suggestions for adaptation of the case, including additional readings and other teaching cases to help students better understand and complete the case.
4. Discussion notes to introduce the internal control frameworks.
5. Discussion notes to help students complete the matrices and rate the control issues.
6. A grading rubric.

TEACHING NOTES

Teaching Notes are available only to full-member subscribers to *Issues in Accounting Education* through the American Accounting Association's electronic publications system at http://aaapubs.org/. Full-member subscribers should use their usernames and passwords for entry into the system where the Teaching Notes can be reviewed and printed. Please do not make the Teaching Notes available to students or post them on websites.

If you are a full member of AAA with a subscription to *Issues in Accounting Education* and have any trouble accessing this material, then please contact the AAA headquarters office at info@aaahq.org or (941) 921-7747.

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2006. *Understanding the Entity and Its Environment and Accessing the Risks of Material Misstatement*. Statement on Auditing Standards (SAS) No. 109. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2009. The AICPA's 2009 top technology initiatives. Available at: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TopTechnologyInitiatives/Top10TechnologiesArchive/Pages/2009TTI.aspx

CBS News. 2007. *Hi-Tech Heist: How Hi-Tech Thieves Stole Millions of Customer Financial Records*. Video available at: http://www.youtube.com/watch?v=MxG2J3bf1BQ

Committee of Sponsoring Organizations (COSO). 1992. *Internal Control-Integrated Framework*. New York, NY: AICPA.

Committee of Sponsoring Organizations (COSO). 2004. *Enterprise Risk Management Framework*. New York, NY: AICPA.

Commonwealth of Massachusetts. 2008. 201 CMR 17.00: Standards for the protection of personal information of residence of the commonwealth. Available at: http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

Damianides, M. 2004. How does SOX change IT? *The Journal of Corporate Accounting and Finance* 15 (6): 35–41.

Foster, S. and C. Bolt-Lee. 2002. New competencies for accounting students. *The CPA Journal* 72 (1): 68–71.

Identity Theft Resource Center (ITRC). 2008. Security Breaches 2008. Available at: http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml

Information Systems Audit and Control Association (ISACA). 2007. *Control Objectives for Information and Related Technology*. Available at: http://www.isaca.org

Information Technology Governance Institute (ITGI). 2006. IT control objectives for Sarbanes-Oxley: The role of IT in the design and implementation of internal control over financial reporting, second edition (September). Available at: http://www.isaca.org

Payment Card Industry (PCI) Security Standards Council. 2008. *Payment Card Industry Data Security Standards (DSS), Version 1.2* (October 1). Available at: www.pcisecuritystandards.org

Public Company Accounting Oversight Board (PCAOB). 2007. *An Audit of Internal Controls over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*. Auditing Standard No. 5. Washington, D.C.: PCAOB.

Ridley, G., J. Young, and P. Carroll, 2004. COBIT and its utilization: A framework from the literature. *Proceedings from the 37th Hawaii International Conference on System Sciences*.

Securities and Exchange Commission. 2003. Final rule: Management's report on internal control over financial reporting and certification of disclosure in Exchange Act periodic reports. Available at: http://www.sec.gov/rules/final/33-8238.htm

U.S. House of Representatives, 2002. The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H.R. 3763]. Washington, D.C.: Government Printing Office. Available at: http://www.sec.gov/about/laws/soa2002.pdf