Exploring the Impact of IT Capability on IT Control: An Information Compliance Approach

Shi-Ming Huang
Department of Accounting and Information Technology
National Chung Cheng University, Chia-Yi, Taiwan

Chia-Sheng Hung*
Department of Accounting and Information Science
Nan Hua University, Chia-Yi, Taiwan

J. Michael Tarn
Department of Business Information Systems
Western Michigan University, Kalamazoo, MI 49008, USA

Mei-Yi Cheng
Department of Accounting and Information Technology
National Chung Cheng University, Chia-Yi, Taiwan

Corresponding Author: eco0303@gmail.com

ABSTRACT

This research aims to investigate the relationship between the IT capability of an enterprise (in terms of IT infrastructure, IT human resources, and intangible IT-enabled resources) and the extent of IT control regulated by the Sarbanes-Oxley Act. The empirical results show evidence of the positive and significant relationship between the IT capability and the extent of IT control regulated by the Sarbanes-Oxley Act. There is little research investigating enterprise IT capability and IT control under the concept of information compliance. To enhance the extent of IT control regulated by the Sarbanes-Oxley Act, business enterprises should highlight the importance of IT capability and the auditing of systems. The enterprises should enhance their employees' understanding of corporate operations and improve the managerial ability of their IT divisions so that the more qualified and suitable management and IT can be developed to help meet the requirements of the Sarbanes-Oxley Act.

Keywords: IT Capability, Control, Governance, Information Compliance, Sarbanes-Oxley

Acknowledgements: Partial funding support for this research was provided by (1) South Asia and China Education Program (SACEP), a BIE grant from the U.S. Department of Education, and (2) National Science Foundation, Taiwan (Grant number: NSC-96-2416-H-194-007-MY3).

INTRODUCTION

The Anderson-Enron lesson was a painful reminder of the need for information reliability and corporate accountability. Such egregious failings in corporate governance and ethics left us shocked and wondering how these scandals were possible and what needed to be done to prevent such failures in the future. The US Congress took its mandate to pass legislation to protect investors and employees from such abuses. Specifically, the Sarbanes-Oxley Act of 2002 (SOX) was intended to reduce the likelihood of further corporate scandals by setting new standards for corporate control and governance. The law is large and far-reaching and further adds to the complex regulatory environment that companies must continually navigate. Although many business organizations have invested a great deal of money in information compliance, it was not immediately clear what the post-SOX business landscape would look like and how companies would respond to the requirement of information compliance. This initiated the previous research on examining the effect of information compliance on the business process of area firms in the US from an Information Technology (IT) perspective (Carrign, 2005).

The stated research then triggers a desirable research study in investigating the relationship between IT capability and IT governance of an enterprise. The rationale is that under SOX, companies must establish perfect internal control systems to ensure that their financial statements are accurate and trustful. In other words, corporate operations rely on information technology to a much greater extent. Information control becomes an important component of internal control. According to ITIG(2006), in order to comply with SOX enterprises should take advantage of IT to monitor and support the processes of internal control and financial reporting and assure the effectiveness of information control.

The challenges CIOs may face include documenting the relevant knowledge and plans for SOX and achieving information control effectively. Hence, some research studies see the compliance with SOX as the effective implementation of information control (Bielski, 2004; Damianides, 2005). Carrigan (2005) claims that SOX has a significant impact on business processes which are supported by information technology, so the ability of information technology is a critical factor to complying with SOX. Bharadwaj (2000) defines information technology capability as the ability to organize, integrate and apply the resources of information technology. For the relevant empirical studies, the focuses are the impacts of SOX on corporate governance and the relation between the ability of information technology and corporate performance.

The risks that companies face in Taiwan are similar to those that American companies face. Those business companies who understand both the opportunities and the risks are those who will profit. Nevertheless, to ensure the development of a healthy economy in Taiwan, a robust IT infrastructure needs to be extended to business companies so that the ultimate goal of information compliance can be achieved. It should be noted that the Taiwanese government has taken a similar compliance approach like SOX to guide and regulate its business companies.

Currently, there is little research investigating enterprise IT capability and IT control under the concept of information compliance. However, research reports suggest that business enterprises have significantly invested in increasing their IT capabilities to achieve the goal of IT control and comply with the requirements of SOX. This study therefore aims to investigate the relationship between the IT capability (in terms of IT infrastructure, IT human resources, and intangible IT-enabled resources) and the extent of

IT control regulated by SOX. The research will take an empirical approach to examining the impact of IT capability on IT control in compliance with SOX in Taiwan. Then the relationships tested can be used to diagnose the maturity of the overall corporate IT infrastructure and resources. Further, the effectiveness of corporate IT control in compliance with SOX can be tested by the IT capability of an enterprise in terms of its IT infrastructure, intangible IT-related resources, and human IT recourses. Not only will the results help Taiwanese companies improve their IT-driven business operations, but they also will assist multinational enterprises in formulating their foreign expansion strategies in Taiwan.

This article consists of six sections. The following section provides the literature background of the study. The research model and hypotheses are presented in Section 3. Section 4 discusses the research method and Section 5 is the analysis of the empirical results. The study is concluded in Section 5.

BACKGROUND AND LITERATURE REVIEW

SOX, IT Governance and Information Compliance

SOX is one of the most important legislation affecting listed corporations on the US stock markets, since the Securities Act of 1933 and Securities Exchange Act of 1934 were enacted. Section 302 of SOX is titled as "Corporate Responsibility for Financial Reports". This section requires the CEO and CFO to take personal responsibility for establishing and maintaining the corporation's internal controls and for certifying that the financial statements provide an accurate representation of a corporation's financial condition. Section 404 of SOX, entitled "Management Assessment of Internal Controls," requires the annual reports filed with SEC to include an internal control report which states the responsibility of management and contains an assessment of the effectiveness of internal control.

Graham, Harvey, &Rajgopal (2008) provide evidence that CFOs believe that SOX affects corporate risk-taking by altering compensation incentives. Cohen, Dey, & Lys (2007) show that SOX reduces the use of stock options in executive compensation plans.Linck, Netter, & Yang (2008) find that boards of publicly traded US corporations are larger and consist of more outside directors after SOX. Bargeron, Lehn, &Zutter (2009) propose that SOX affects corporate risk-taking in two ways. First, SOX discourages officers and directors form initiating and approving risk investment projects by expanding the role played independent directors and imposing more liability (including criminal liability). Second, Section 404 which requires companies to test and disclose the adequacy of their internal controls, is expected to have a discouraging effect on corporate risk-taking. Though SOX does not explicitly address the issue of information security, Gordon, Loeb, Lucyshyn, &Sohail (2006) find the evidence that SOX has positive impact on the voluntary disclosure of information security activities of organizations. Chai, Kim, &Rao(2011) examines the value of an investment in IT security, based on stock market investor's reaction toward a firm's IT security investment announcements. The findings indicate stock market reaction to security investments shows higher abnormal returns after SOX than any of those before it.

Controlling and securing information technology within a corporation used to be a nicety. Whereas effective governance over IT has become law after SOX enacted. Bowen,

Cheung, & Rohde (2007) view IT governance as the IT related decision making structure and methodologies implemented to plan, organize, and control IT activities. Sohal& Fitzpatrick (2002) clarified the concepts of IT management and IT governance. They suggested that management is about the making of operating decisions and governance is referred to as the internal governance processes of an organization. Governance is the creation of a setting in which others can manage effectively. So governance answers the question of what must be done. Applied to IT, IT governance decides on what must be arranged in order for the organization to profit from IT synergy. Hence, some research views IT governance is the responsibility of the board of directors and executive management (Hardy, 2006).

SOX requires that organizations implement an appropriate internal control framework such as COSO, but SOX did not endorse a specific IT control framework. Hardy (2006) and Bowen et al. (2007) propose that Control Objectives for Information and related Technology (COBIT) aligns well with SOX compliance efforts.

Information compliance can be approached from many different directions, such as from an accounting perspective, a risk management perspective, or a technological perspective. The first approach, an ethics focus, sees the problems of compliance as inextricably intertwined with the issue of ethics (Gaumnitz, 2004; Ratnatunga&Alam, 2011; Verschoor, 2004). SOX was enacted in the wake of major accounting scandals and is largely aimed at preventing such meltdowns in the future by enforcing stricter scrutiny and documentation of internal company controls. A practical school of research describes information compliance as the implementation of tight information technology controls (Bielski, 2004; Damianides, 2005). From this point of view, SOX is largely about ensuring the integrity of business information, and the IT department is the guardian of this information. Therefore, compliance must mean having proper safeguards in place to guard information and ensure data integrity. Research studies such as "Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance" (Damianides, 2005) take this approach and provide an IT control framework as a basis for SOX compliance.

A Governance, Risk Management, and Compliance management approach toward compliance is similar to an IT controls focus, but is broader (Farrell, 2003; Gincel, 2004; Quall, 2004; Keefe &Tipgos, 2006). This approach advocates using a control framework for the entire organization, rather than only the IT area, as a basis for compliance. A technology tools approach views compliance as a problem that can largely be solved with the proper technology. This may be by implementing the right storage hardware for meeting documentation holding regulations, or buying a piece of software specifically designed to aid with SOX compliance (Daks, 2011; Lanza, 2004; Meyer, 2003; Parson, 2005; Shih, 2010;).

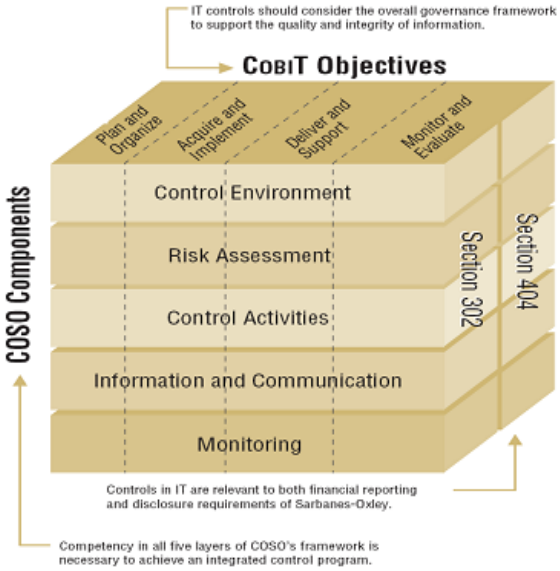
An internal auditing approach views SOX compliance from an accounting perspective, and frames the problem as one that can be solved with greater internal auditing to ensure the integrity of financial information (IAA, 2004). The final approach to SOX compliance advocates a broad aspect of compliance as part of the general business process improvement (Farrell, 2003; Quall, 2004). A narrow view of compliance is one in which the goal is in strict compliance with the letters of the laws. In contrast, the broad aspect sees compliance as one part of a larger strategy to increase the value and effectiveness of the companies' processes wherever possible. Many researchers believe that "implementing section 404 presents a great opportunity to enhance the efficiency and value of the company" (Quall, 2004). In recent years we have seen an increase in businesses

researching and developing ways to implement an alternative architecture that supports continuous auditing as well (Kuhn, 2010).

Carrigan (2005) examines the impacts of SOX on enterprise process and claims that the enterprise process should be supported by information technology. And the abilities of information technology are the critical factors of success to comply SOX. Parson Research (2005) indicates that it is helpful to take advantage of the Business Performance Management (BPM) system when enterprises follow the requirements of SOX. The BPM system can help enterprises correctly evaluate the business process and ensure the accuracy of information.

Forrester Research in 2005 finds that the budget for human resource training has the most rapid growth when compared with the other entries of information technology investment. This is because the reasonable framework of information control complements efficient human resources. McDonnell (2005) and the research report of 2005 issued by Deloitte corp. also highlight the importance of the employees' training. The employees have to understand the importance, impact, and associated responsibilities in compliance with SOX. To document for the internal control knowledge is a big challenge for CIOs who should play the leading role to help the enterprises comply with SOX.

Figure 1: The Model for Information Control in Compliance with the Sarbanes-Oxley Act



Source: IT Governance Institute, 2006

The above discussion emphasizes the importance of information control under the requirements of SOX. The result observed was a significant increase in IT expenditure and investment as evidenced in the Forrester Research's report (2005). According to this report, 46% of the investigated CFOs had planned to increase the IT budget. On the other side, the Committee of Sponsoring Organization of the Treadway commission (COSO) promotes a

better internal control which is to ensure the achievement of the effectiveness, efficiency of operation, reliability of financial report, and the compliance of laws. COSO defines five critical elements, including the structure of internal control, the elements of control environment, risk assessment, control activities, information and communication and monitoring. The Information Systems Audit and Control Association (ISACA) proposed the fourth version of Control Objectives for Information and Related Technology (COBIT) in 1996 and provided a standard framework for information control. It is reasonable to follow COSO and COBIT frameworks to implement information control in compliance with SOX. In the following subsections, COSO and COBIT frameworks are reviewed.

COSO

The COSO framework was first introduced in 1992 and was intended to achieve three corporate objectives: the effective and efficient usage of company resources, production of reliable financial reports, and regulatory and legal compliance (Campbell, Campbell & Adams, 2006). COSO requires that internal control be built into an organization's processes for enterprise, and IT governance and states that there are five components that form internal control. Those components are the control environment, risk assessment, control activities, information and communication, and monitoring (ITGI, 2006). The COSO framework is currently being updated to include compliance operations beyond those associated with financial reporting (Dickins, Denise and Houmes, 2011).

The COSO framework contains five components; i.e., control environment, risk assessment, control activities, information and communication, and monitoring respectively. ITGI (2006) explicates the five components as follows:

- **Control Environment:** Control environment creates the foundation for effective internal control, establishes the "tone at the top" and represents the apex of the corporate governance structure. The issues raised in the control environment component apply throughout an organization. The control environment primarily addresses the entity level.
- **Risk Assessment:** Risk Assessment involves management's identification and analysis of relevant risks to achieving predetermined objectives, which form the basis for determining control activities. Risk assessment may occur at the entity level or at the activity level.
- **Control Activities:** Control activities are the policies, procedures and practices that are put into place so that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified.
- **Information and Communication:** COSO states that information is needed at all levels of an organization to run the business and achieve the entity's control objectives. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allow people to carry out their duties, support the other four components of the COSO framework.
- **Monitoring:** Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management. There are two types of monitoring activities: continuous monitoring and separate evaluations.

While COSO emphasizes the importance of IT within the overall control environment, it does not provide details in the design and implementation of specific IT controls for companies. In view of this, the IT governance Institute applied the COBIT framework (2006) with the use of the COSO framework which can assist companies to address the IT control issues in compliance with SOX. According to ITGI (2006), Figure 1 shows the integration of the five COSO control components and the four COBIT objectives with respect to Sarbanes-Oxley. The COBIT framework is discussed next.

COBIT

COBIT is a framework that consists of a collection of documents that are considered the best practices for IT governance. These superior practices are the harmonization of industry experts and are concentrated more on control and less on execution. The framework consists of 34 different processes that are categorized into one of four separate domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate (ITGI, 2006). COBIT is considered to be one of the most comprehensive IT governance methodologies in the industry and is often the standard against which other frameworks are measured. It is evident that many COBIT IT processes have relationships with more than one COSO component. This relationship demonstrates the reason why IT controls are the basis of and are essential for a reliable internal control program.

IT Capability

Resource-based theory posits that firms compete on the basis of unique corporate resources that are valuable, rare, difficult to imitate, and non-substitutable by other resources. Besides, resource availability is a significant factor in enhancing self-efficacy, as well as a significant predictor of policy compliance intentions. Grant (1995) classifies enterprise resources into three types: tangible resources, intangible resources and personnel-based resources. Tangible resources include financial assets and physical capital such as planes, equipment and inventory. Intangible resources fall into reputation, product quality and brand image. As for personnel-based resources, they consist of professional knowledge and intellectual capital such as organization culture, employee training and employee loyalty.

Another approach proposed by Powell & Dent-Micallef (1997) categorizes information resources into three classifications, including human resources, business resources, and technology resources. Feeny&Willcocks (1998) define nine core IS capabilities in four areas, including business and IT vision, design of IT architectures, delivery of IS services, and a core set of capabilities like IS leadership and information buying.

Bharadwaj (2000) follows the classification of Grant (1995) and classifies IT capability as IT Infrastructure, human IT resources, and intangible IT-enabled resource. IT infrastructure is the physical IT asset which comprises computer and communication technologies as well as shareable platforms and databases. Human IT resources include technical IT skills and managerial IT skills. Technical IT skills include programming, system analysis and design, competencies in new technologies, etc. As for managerial IT skills, the effectiveness of IS functions management, organization, coordination and interaction with user communities, project management and leadership skills belong to this category(Bharadwaj, 2000; Copeland & McKenney,1988). Organizational intangible

resources contain environmental orientation, corporate reputation, corporate culture, and corporate know-how (Russo &Fouts, 1997; Teece& Pisano, 1997; Vergin&Qoronfleh, 1998). Intangible IT-enabled resources are specifically referred to as organizational intangibles, such as product quality, customer service, market orientation, knowledge assets, organizational memory, organizational learning, synergy, etc.

Li ,Heck and Verest (2009) investigate how mobile ticketing technologies can enable revenue management. They propose that IT capability as a firm's ability to capture the complete customer behavior information. Masli, Richardson, Sanchez, &Smith (2010) examine the impact of superior IT capabilities on firm performance over the 1988-2007 period. They propose that the firms with high levels of IT capabilities perform better than their peers and managers are able to achieve superior firm performance if they are able to maintain high levels of IT capability over time. Ortega (2010) study the moderating roles of IT capabilities and find that IT capabilities enhance the relationships between quality orientation and performance, and cost orientation and performance, respectively.

Recent researches focus on the enabling role of IT capability which improves the business agility (Gimun, 2011; Oosterhout, Waarts, &Hillegersberg 2006; Overby, Bharadwaj,&Sambamuthy, 2006). Some studies argue that IT assets are the easiest resources to be replicated by competitors, which become the weakest source of sustainable competitive advantage for an organization (Teece& Pisano, 1997). Nevertheless, Byrd & Turner (2000) argues that a responsive and flexible IT infrastructure can increase competitive advantage of adopting organizations.

Further, more researchers believe that an organization's competitive advantages can be created though organization capabilities (Byrd, 2010; Christensen &Overdorf, 2000) and intangible assets (Hall, 1997; Srivastava, Shervani, & Fahey, 1998). According to Huang, Ou, Chern, & Lin (2006), IT infrastructure and firm performance do not have a direct relationship. However, IT infrastructure and human IT resources influence IT-enabled intangible assets significantly, while IT-enabled intangible assets positively impact on the firm's performance. Because a company's IT-enabled intangible assets can be enhanced via the improvement of IT infrastructure and human IT resources, the company is suggested to consider investing in both mentioned dimensions to improve its IT resources and performance more effectively. Firms are more and more looking at the relationship between IT capabilities, process-oriented dynamic capabilities, and financial performance to increase firm performance (Gimun, 2011).In summary, the above discussion will serve as the base for the development of the research model and hypotheses.

RESEARCH MODEL AND HYPOTHESES

Research Hypotheses

According to the literature review, it can be reasonably expected that the enterprises which possess better IT capability can implement information control better in compliance with SOX. The following propose the main hypotheses:

Hypothesis1 ： IT capability is positively related with corporate IT control in compliance with SOX.

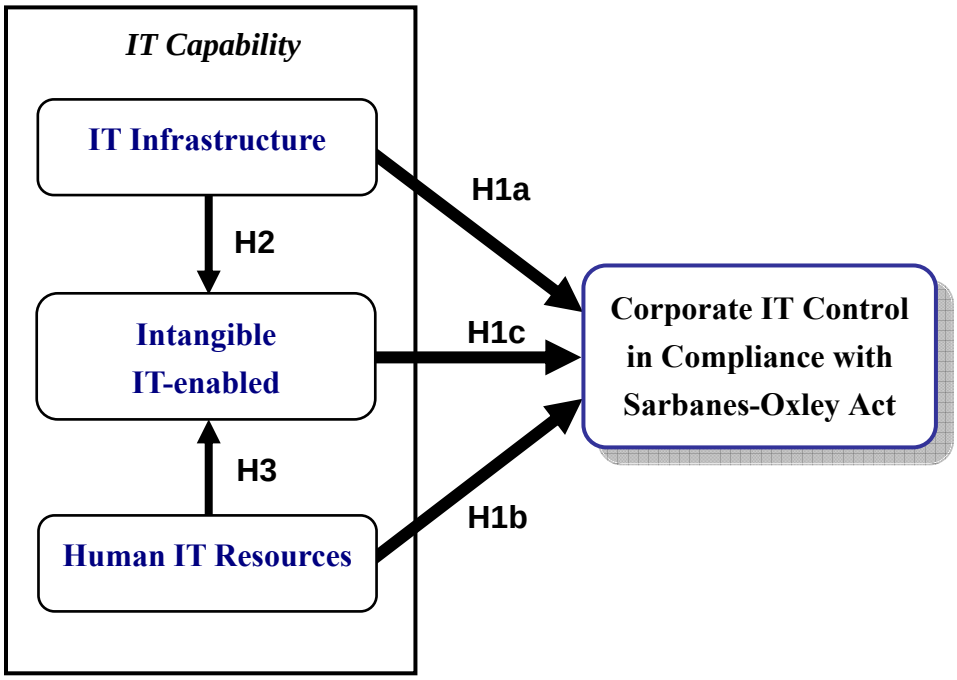
Because IT capability is classified as IT Infrastructure, human IT resources and intangible IT-enabled resources, the above hypothesis can be tested via the following three sub-hypotheses.

Hypothesis 1a：IT Infrastructure is positively related to corporate IT control in compliance with SOX.

Hypothesis 1b：Human IT resources are positively related to corporate IT control in compliance with SOX.

Hypothesis 1c：Intangible IT-enabled resources are positively related to corporate IT control in compliance with SOX.

Figure 2: Research Model



Intangible IT-enabled resources as organizational intangibles include knowledge assets and synergy. Knowledge assets can accrue competitive advantages via information systems to share and integrate knowledge within an enterprise (Brown &Duguid, 1998; Matusik& Hill, 1998). Synergy stands for the advantages derived from resources sharing and capabilities integrated within an enterprise. Brown et al. (1998) argue that IT Infrastructure and human IT resources are the bases when it comes to achieving synergy. Therefore, it can be hypothesized that IT Infrastructure and human IT resources are positively related with intangible IT-enabled resources. The hypotheses are listed below.

Hypothesis 2：IT Infrastructure is positively related to intangible IT-enabled resources.

Hypothesis 3：Human IT resources are positively related to intangible IT-enabled resources.

Research Model

The research model is shown in Figure 2. This research will examine the relationship between IT capability, in terms of IT Infrastructure, human IT resources and intangible IT-enabled resources, and IT control under the norm of SOX. The relationships between IT infrastructure, human IT resources, and intangible IT-enabled resources will also be examined.

Research Method

Questionnaire design and measurements

A survey approach is adopted in this research project. The content and framework of questionnaires to measure IT capability refers to Byrd et al. (2000), Bharardwaj (2000), and Huang et al. (2006). A content evaluation panel which contains 12 experts was formed to review the items. The content evaluation panel included two professors, two senior managers of computer audit department, and eight CIOs. Based on Lawshe (1975)'s validation method, the questionnaire is reviewed by experts to ensure the validity of the contents. There are fifteen variables for IT Infrastructure, sixteen variables for human IT resources and four variables for intangible IT-enabled resources. The measurement of IT Control in compliance with SOX adopts the questionnaire of IT Control Objectives for Sarbanes-Oxley (2nd Edition, 2006) proposed by the IT Governance Institute. Generally speaking, IT control includes the Entity Level Controls and Activity Level Controls. The entity level controls are concerned with the entire operating and organizational culture within an enterprise, which is helpful for top management to evaluate the degree of IT control. Since this study adopts and investigates IT control from the aspect of entity level controls, the questionnaire employs the four entity level control dimensions of the COSO framework; namely control environment, risk assessment, information and communication, and monitoring. The measurement of independent variables uses Likert's 5-point scale, and the dependent variable uses Likert's 3-point scale.

Sampling and data collection

The investigating samples are 331 companies that are members of the Association of Industries in Science Parks in Taiwan. The questionnaires were answered by the CIO or the head of the computer auditing related department. The pilot test was implemented by three IT auditors who come from the traditional, electronic and financial industries, respectively. There were 110 completed surveys returned, which are equivalent to the response rate of 33.23%. The basic statistics are shown in Table 1. Table 2 compares the degree of IT control under different basic settings.

Table 1: Basic Data from the Respondent Companies

Question	Content	Number of samples	Percentage
Interviewees' titles	Chief of information Chief of computer auditing	80 22	78.4 21.6
Number of employees	Below 100 101-1000 1001-2000 2001-5000 Above 5000	5 49 24 8 16	4.9 48.0 23.5 7.8 15.7
Number of employees in information related department	Below 10 11-25 26-50 51-100 Above 101	52 27 13 7 3	51.0 26.5 12.7 6.9 2.9
There is a specific department for computer auditing	Yes No	23 79	22.5 77.5
There are some specific employees for computer auditing	Yes No	50 52	49.0 51.0
There is certain application software for internal control and computer auditing	Yes No	31 71	30.4 69.6
Checked by external units for the process of information control	Yes No	79 23	77.5 22.5
It is necessary to comply with Sarbanes-Oxley Act	Yes No	25 77	24.5 75.5
Required to comply Sarbanes-Oxley Act by customers and suppliers	Yes No	29 73	28.4 71.6
Checked by external units for implementing Section 404 of Sarbanes-Oxley Act	Yes No	17 85	16.7 83.3

\

DATA ANALYSIS AND MODEL VALIDATION

Before conducting the path analysis to validate the research model, we confirmed the reliability and validity of the collected data. As a general rule, the reliability is good if the

Cronbach's α is higher than 0.7. Table 3 shows the Cronbach's α for the three dimensions of IT capability and four dimensions of IT control. The Cronbach's α for both IT capability and IT control dimensions are all higher than 0.7. In other words, the measurements of IT capability and IT control are reliable and valid.

Table 2: The Degree of IT Control

Basic Questions		The degree of information technology control	
		Average Score	T value
There is a specific department for computer auditing	Yes	59.91	3.755**
	No	51.63	
There are some specific employees for computer auditing	Yes	58.80	6.218**
	No	48.40	
There is certain application software for internal control and computer auditing	Yes	58.74	3.760**
	No	51.21	
Checked by external units for the process of information control	Yes	55.84	4.896**
	No	45.48	
It is necessary to comply the Sarbanes-Oxley Act	Yes	62.92	6.506**
	No	50.44	
Required to comply the Sarbanes-Oxley Act by customers and suppliers	Yes	56.62	2.040*
	No	52.26	
Checked by external units for implementing Section 404 of Sarbanes-Oxley Act	Yes	64.94	6.085**
	No	51.21	

* $p<0.05$ ** $p<0.01$

Table 3: The Cronbach's α of IT Capability and IT Control

IT Capability	**Cronbach's α**
IT Infrastructure	0.911
Human IT resources	0.920
Intangible IT-enabled resource	0.859
IT Control	
Control Environment	0.890
Information and Communication	0.787
Risk Assessment	0.805
Monitoring	0.873

In order to ensure that the collected data is suitable for factor analysis, the Bartlett's test of sphericity and the KMO (Kaiser-Meyer-Olkin) test are performed. The results show that the KMO of IT Infrastructure, human IT resources and intangible IT-enabled resource are 0.866, 0.884 and 0.823, respectively. The values of Bartlett's test of sphericity are 846.329, 986.669 and 213.569, respectively, which prove that the data is suitable for factor analysis.

Table 4: The Results of Principal Component Analysis

Factor	Name	Number of Questions	Eigen value	Explanatory Power (%)	Cumulative Explanatory Power (%)	Cronbach's α
IT infrastructure						
FFC1	Systems integration and connectivity	7	6.827	45.513	45.513	0.872
FFC2	System and network auditing and control	4	1.773	11.554	57.067	0.888
FFC3	System compatibility	4	1.021	6.809	63.877	0.768
Human IT resources						
FHR1	Understanding of corporate operations	8	7.513	46.957	46.957	0.888
FHR2	Capacity of teamwork	5	1.677	10.479	57.436	0.904
FHR3	Managerial ability of IT division	3	1.437	8.982	66.418	0.787
Intangible IT-enabled resources						
FI1	Capability of corporate knowledge management	4	2.938	73.445	73.445	0.859

Therefore, the principal component analysis is further conducted to reduce the number of variables to ensure the construct validity of IT capability. The variables whose eigen value and loading are larger than 1 and 0.5 respectively are selected (Hair, 1998). The results of principal component analysis are presented in Table 4. The fifteen variables in IT Infrastructure dimension are integrated as three factors and denoted as FFC1 (system integration and connectivity), FFC2 (system and network auditing and control), and FFC3 (system compatibility). The Eigen values of these three integrated factors are larger than one, and the total explanatory Power is up to 63.877%. The sixteen variables in human IT resources dimension are integrated as three factors and denoted as FHR1 (degree of

understanding of corporate operations), FHR2 (capacity of teamwork), and FHR3 (managerial ability of IT division). The Eigen values of these three integrated factors are also larger than one, and the total Explanatory Power is 66.418%. The four variables in the dimension of intangible IT-enabled resources are integrated as one factor and denoted as FI1 (capability of corporate knowledge management). The Eigen value of this integrated factor is 2.938, and the total Explanatory Power is 73.445%. The Cronbach's α of integrated factors are located from 0.787 to 0.904.

Table 5 shows the test of independent variables for normality assumption. By checking the Z-value of skewness and kurtosis, we find that two variables, FFC1 and FHR2, do not meet the normality assumption. We take the square values of these two variables for empirical study to meet the normality assumption. Table 6 shows the Pearson's coefficients of correlation. All values of the coefficients of correlation are below 0.8, this means that there is no significantly colinearity existing between variables (Hair, 1998).

Table 5: The Results of Normality Test

Factors	Number	Skewness			Kurtosis		
		Statistic	Std. Error	Zs	Statistic	Std. Error	Zk
FFC1	102	-.911	0.239	-3.755	1.555	0.474	3.205
FFC2	102	-0.621	0.239	-2.383	1.046	0.474	2.157
FFC3	102	0.083	0.239	0.344	-0.857	0.474	-1.767
FHR1	102	-0.363	0.239	-1.498	-0.451	0.474	-0.930
FHR2	102	-0.140	0.239	-0.578	-0.245	0.474	-0.505
FHR3	102	-0.650	0.239	-2.681	2.021	0.474	4.167
FI1	102	-0.240	0.239	-0.989	0.407	0.474	0.840

Table 6: The Coefficients of Correlation

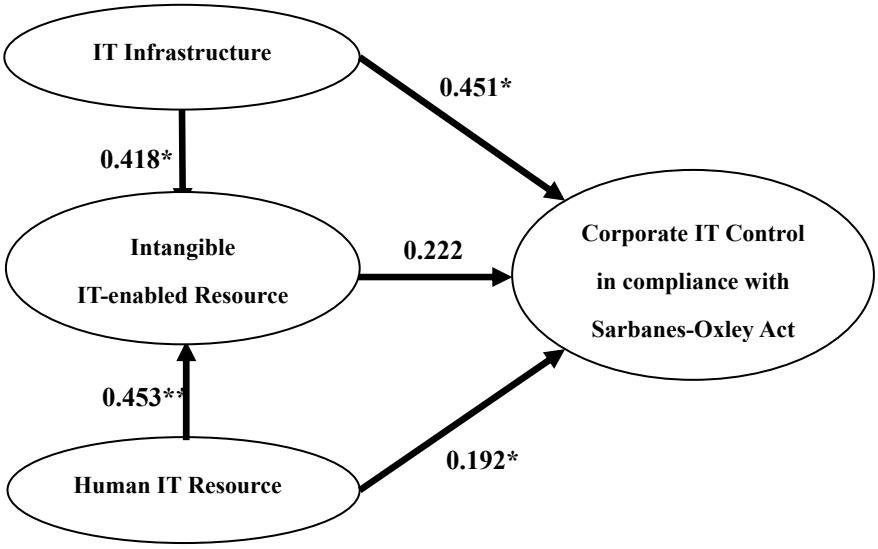
Factors	FFC1	FFC2	FFC3	FHR1	FHR2	FHR3	FI1
FFC1	1.000						
FFC2	**0.599**	1.000					
FFC3	**0.584**	**0.337**	1.000				
FHR1	**0.452**	**0.544**	**0.414**	1.000			
FHR2	**0.501**	**0.403**	**0.335**	**0.629**	1.000		
FHR3	**0.317**	**0.379**	**0.377**	**0.412**	**0.452**	1.000	
FI1	**0.608**	**0.675**	**0.438**	**0.669**	**0.579**	**0.475**	1.000

Table 7: The Empirical Results of Path Analysis

Panel A: the empirical results of IT infrastructure, Human IT resource and intangible IT-enabled resource Dependent variable: Intangible IT-enabled resource			
Independent variables	β	t-value	VIF
IT infrastructure	0.418**	5.254	1.637
Human IT resources	0.453**	5.687	1.637
R-SQUARE=0.616 Durbin-Watson=2.157			
Panel A: the empirical results of IT capability and IT Control in compliance with Sarbanes-Oxley Act. Dependent variable: IT Control in compliance with Sarbanes-Oxley Act			
Independent variables	β	t-value	VIF
IT infrastructure	0.451**	4.875	2.093
Human IT resources	0.192*	2.042	2.171
intangible IT-enabled resources	0.222*	2.147	2.171
R-SQUARE=0.599 Durbin-Watson=1.878			

*: p<0.05 **: p<0.01

Figure3: The Empirical Results of the Path Analysis (*: p<0.05 **: p<0.01)



According to the path analysis, we first investigate the relationship between IT infrastructure, Human IT resources and intangible IT-enabled resources, and then

investigate the relationship between IT capability and IT Control. Table 7 shows the empirical results. Panel A is the result between IT infrastructure, Human IT resources and intangible IT-enabled resources. The standardized coefficients of IT infrastructure and Human IT resources are 0.418 and 0.453, respectively. The corresponding t-values of these two independent variables are 5.254 and 5.687. Hence, intangible IT-enabled resources are positively and significantly affected by IT infrastructure and Human IT resources. The VIF of IT infrastructure and Human IT resources are both 1.637. No evidence supports that there is colinearity between IT infrastructure and Human IT resources. These empirical results provide evidence for supporting hypotheses 2 and 3. Panel B shows the relationship between IT capability and IT control. The standardized coefficients of IT infrastructure, Human IT resources and intangible IT-enabled resources are 0.451, 0.192 and 0.222, and the corresponding t-values are 4.875, 2.042 and 2.147. The VIF of IT infrastructure, Human IT resources and intangible IT-enabled resources are 2.093, 2.171 and 2.171. All coefficients are significantly different from zero. These results suggest that the IT infrastructure, Human IT resources and intangible IT-enabled resources are positively affecting IT control. The hypotheses are supported by these results.

Figure 3 illustrates the empirical results of the path analysis. IT control is positively and significantly affected by the three dimensions of IT capabilities; i.e., IT infrastructure, Human IT resources, and intangible IT-enabled resources. Moreover, intangible IT-enabled resources are positively and significantly impacted by infrastructure and Human IT resources.

CONCLUSION

In this section, two conclusions are to be addressed. The first is about the implications of IT capability, and the other concerns the impact of IT capability on IT control in compliance with SOX. In terms of IT capability, this research identifies certain important factors from the factor analysis. The three factors in IT infrastructure are system integration and connectivity, system and network auditing and control, and system compatibility. In the aspect of human IT resources, the three factors identified are the degree of understanding of corporate operations, the capacity of teamwork, and the managerial ability of IT division. And in the aspect of intangible IT-enabled resource, a factor – the capability of corporate knowledge management – is identified. The implications of these factors would direct business enterprises toward the better IT capability for improving their business processes and operations.

By taking advantage of the path analysis and stepwise regression, we found that a company's IT infrastructure and human IT resources would have significant influence on its intangible IT-enabled resources. Further, the system and network auditing and control, degree of understanding of corporate operations, and managerial ability of IT division are the most influential factors. With respect to the relationship between IT capability and IT control, IT infrastructure and human IT resources, and intangible IT-enabled resources all have a significant impact on IT control. The system and network auditing and control, degree of understanding of corporate operations, and system integration and connectivity are the most influential factors.

In summary, the hypotheses H1a, H1b, and H1c are well supported by the empirical results. That is, IT Infrastructure, human IT resource, and intangible IT-enabled resources are positively related with the SOX-based corporate IT Control. Besides, the empirical results support the hypotheses H2 and H3. Hence, IT Infrastructure and human IT

resources are positively related with intangible IT-enabled resources. These results are consistent with the findings of Bharadwaj (2000) and Huang et al. (2006).

In order to comply with SOX, business companies should highlight the importance of IT capability and the auditing of systems. In addition, they should enhance their employees' understanding of corporate operations and improve the managerial ability of their IT divisions. In this sense, the company can develop more qualified and suitable management and IT systems that can help to meet the requirements of SOX. Lastly, this study focused on the relationship between IT capability and IT control. The causal relationship between corporate performance and IT capability and IT control were not investigated, which should provide a valuable direction for future research.

REFERENCES

Bargeron, L. L., Lehn, K. M.,& Zutter, C. J. (2010). Sarbanes-Oxley and corporate risk-taking,*Journal of Accounting and Economics*, 49: 34-52.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation,*MIS Quarterly*, 24(1): 169-196.

Bielski, L. (2004). Keep proprietary information in its place. *ABA Banking Journal*, 96(4): 53-58.

Brown, J. S. & Duguid, P. (1998).Organizing Knowledge.*California Management Review*, 40(3): 90-111.

Bowen, P. L., Cheung, M. Y. D., & Rohde, F. H. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. International Journal of Accounting Information Systems, 8(3): 191-221.

Byrd, L. W.& Byrd, T. A. (2010).Contrasting IT capability and organizational types: implications for firm performance,*Journal of Organizational and End User Computing*, Oct-Dec.

Byrd, T. A. & Turner, D. E. (2000). Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct.*Journal of Management Information Systems*, 17(1): 167-208.

Campbell, D. M. & Campbell, G. A. (2006).Adding Significant Value with Internal Control.*The CPA Journal*, 76(6): 20-26.

Carrigan, J. (2005). *Exploring the Impact of Sarbanes-Oxley and Information Compliance on Organizational Business Process*. Honors Thesis, Western Michigan University.

Chai, S., Kim, M. & Rao, H.R. (2011). Firms' information security investment decisions: Stock market evidence of investor's behavior, *Decision Support Systems*. 50: 651-661.

Christensen, C. M., & Overdorf, M. (2000). Meeting the Challenge of Disruptive Change.*Harvard Business Review*, 78(2): 67-75.

Cohen, D. & Dey, A. Lys, T. (2007). The Sarbanes-Oxley Act of 2002: implications for compensation contracts and managerial risk-taking, Northwestern University.

Copeland, D. G., & McKenney, J. L. (1988). Airline Reservation Systems: Lessons from History. *MIS Quarterly*. 12(3): 353-370.

Daks, M. C. (2011). Accountants: Software Creates Less-Taxing Environment. *NJBIZ*, 24(31): 18-22.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT controls and compliance, *Information Systems Management*, 22(1): 77-84.

Dickins, D.. & Houmes, R. (2011). Coso Framework Changes.*Internal Auditing*, 26(5): 37-41.

Farrell, J. (2003). A broad view of section 404.*The Internal Auditor*. 60(4): 88.

Farrell, J. (2003). Internal controls and managing enterprise-wide risks.*The CPA Journal*, 74(8): 11-12.

Feeny, D. F., & Willcocks, L. P. (1998). Core IS Capabilities for Exploiting Information Technology.*Sloan Management Review*, 39(3): 9-21.

Gaumnitz, B. R. (2004). Codes of ethics with impact.*The CPA Journal*, 74(5): 64-67.

Kim, G. (2011). IT Capabilities, Process-Oriented Dynamic Capabilities, and Firm Financial Performance.*Journal of the Association for Information Systems*, 12(7): 487-517.

Gincel, R. (2004). The Feds are watching. Are you ready? *InfoWorld*, 26:32-38.

Gordon, L.A., Loeb, M. P., Lucyshyn, W., & Sohail, T (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25:503-530.

Graham, J, Harvey, C., & Rajgopal, S. (2008). *The economic value versus reported earnings trade-off and voluntary disclosure*.Duke University.

Grant, R. M. (1995). *Contemporary Strategy Analysis*, Blackwell Publishers, Oxford, UK.

Hair, J. F,, Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate Data Analysis.Computers & Security. 21(2): 172-192.

Hall, R. (1997). *Complex Systems, Complex Learning, and Competence Building*.New York, Wiley.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11: 55-61.

Huang, S. M., Ou, C. S., Chern C. M., & Lin, B. (2006). An Empirical Study of Relationship between IT Investment and Firm Performance: A Resource-Based Perspective. *European Journal of Operational Research*.173(3): 984-999.

Institute of International Auditors (IIA) (2004). Internal auditing's role in sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002. Altamonte Springs, FL.

ITGI (2006). COBIT Mapping: Overview of International IT Guidance (2nd Edition), IT Governance Institute, Rolling Meadows, IL.

ITGI (2006). IT Control Objectives for Sarbanes-Oxley, The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, IT Governance Institute.

Keefe, T. J., & Tipgos, M. A. (2004). A comprehensive structure of corporate governance in post-Enron corporate America.*The CPA Journal*, 74(12): 46-51.

Kuhn, J.R., & Sutton, S. G. (2010). Continuous Auditing in ERP System Environments: The Current State and Future Directions.*Journal of Information Systems*, 24(1): 91-112.

Lanza, R. B. (2004). Making sense of Sarbanes-Oxley tools. *The Internal Auditor*, 61(1): 45-51.

Lawshe, C. H. (1975). A quantitative approach to content validity.*Personnel Psychology*, 28: 563-575.

Li, T., Heck, E.,Verest, V. P. (2009). Information capability and value creation strategy: advancing revenue management through mobile ticketing technologies. *European Journal of Information Systems*, 18: 38-51.

Linck, J. S., Netter, J. M., & Yang, T. (2008). The determinants of board structure.*Journal of Financial Economics*, 87(2): 308-328.

Masli, A., Richardson, V. J., Sanchez, J.M., & Smith, R.E. (2011). Returns to IT excellence: Evidence from financial performance around information technology excellence awards.*International Journal of Accounting Information Systems*, 12: 189-205.

Matusik, S. F., & Hill, C. W. (1998). The Utilization of Contingent Work, Knowledge Creation, and Competitive Advantage.*The Academy of Management Review*, 23(4): 680-697.

McDonnell, P. J. (2005). The PCAOB and the Future of Oversight.*Journal of Accountancy*, 198 (6): 98-101.

Meyer, M. (2003). Corporate real estate and Sarbanes-Oxley: Web-based tools for ensuring compliance and improving financial management*. Journal of Corporate Real Estate*, 6(1): 83-92.

Oosterhout, M. V., Waarts, E. J., & Hillegersberg, V. (2006). Change factors requiring agility and implications for IT. *European Journal of Information Systems*, 15: 132-145.

Ortega, M. J. R. (2010). Competitive strategies and firm performance: Technological capabilities' moderating roles. *Journal of Business Research*, 63: 1273-1281.

Overby, E., Bharadwaj, A., & Sambamurthy, V. (2006).Enterprise agility and the enabling role of information technology.*European Journal of Information Systems*, 15: 120-131.

Parson Research (2005). Sarbanes-Oxley Effect: Caution on Guidance, Financial Executive, 10.

Powell, T. C., & Dent-Micallef, A. (1997). Information technology as competitive advantage: The role of human, business, and technology resources. *Strategic Management Journal*, 18(5): 375-405.

Quall, J. C. (2004). Implementing section 404: A practical approach to the Sarbanes-Oxley act.*The CPA Journal*, 74(8): 52-59.

Ratnatunga, J., & Alam, M. (2011). Strategic Governance and Management Accounting: Evidence from a Case Study. *Abacus*, 47: 343–382.

Russo, M. V., & Fouts, P. A. (1997). A resource-based perspective on corporate environmental performance and profitability.*Academy of Management Journal*, 40(3): 534-559.

Shih, K. H. (2010). Risk Indicators for Computer Systems Assisted Financial Examination.*The Journal of Computer Information Systems*, 50(4): 97-106.

Sohal, A., & Fitzpatrick, S. P. (2002). IT governance and management in large Australian organizations.*International Journal of Production Economics*, 75: 97-112.

Srivastava, R., Shervani, K. T., & Fahey, A. L. (1998).Market-Based Assets and Shareholder Value: A Framework for Analysis. *Journal of Marketing*, 62(January): 2-18.

Teece, D. J., & Pisano, G. A. (1997). Dynamic capabilities and Strategic Management.*Strategic Management Journal*, 18(7): 509-533.

Vergin, R. C., & Qoronfleh, M. W. (1998). Corporate Reputation and the Stock Market.*Business Horizons*, 41(1): 19-26.

Verschoor, C. C. (2004). Survey shows need for more ethics awareness. *Strategic Finance*, 86(6): 15-16.

Shi-Ming Huang received his PhD degree at the School of Computing and Information Systems, University of Sunderland, U.K. He is currently a Director for the Research Center of e-Manufacturing and e-Commerce at National Chung Cheng University, Taiwan. He has

published five books, three business software and over 70 articles in refereed information system journals, such as *Information and Management*, *Decision Support Systems*, *Journal of Computer Information Systems*, *European Journal of Operational Research*, *Journal of Database Management*, *ACM SIGMOD*, etc. He has received over 10 achievement awards in information system area. He has served as editorial board members in several international journals and has acted as a consultant for a variety of Taiwangovernment departments, software companies and commercial companies.

Chia-Sheng Hung, Associate Professor of Accounting and Information Science at Nanhua University, Chiayi, Taiwan, earned his Ph. D. in International Economics as well as in Accounting at National Chung Cheng University, Taiwan. His recent research interests are IT control, IT investments and performance/cost behavior, and application of data mining. His publications have appeared in *Journal of Engineering and Technology Management, Australian Journal of Educational Technology, International Journal of Management Theory and Practice, Advances in Accounting.*

J. Michael Tarn is Professor and Chair of the Department of Business Information Systems at the Haworth College of Business, Western Michigan University. He holds a Ph.D. and an M.S. in Information Systems from Virginia Commonwealth University. Dr. Tarn has published numerous research articles in refereed journals, book chapters and refereed conference proceedings. He specializes in multidisciplinary research and his areas of expertise are information security management, enterprise systems, networking and data communications, Internet research, IT globalization, and critical systems management. Professor Tarn coauthored the first scholarly book in Enterprise Systems Education, *Enterprise Systems Education in the 21st Century*. He is Editor-in-Chief of the *International Journal of Management Theory and Practices*. He is also former President of the International Chinese Information Systems Association and past Editor-in-Chief of *Communications of the ICISA–an International Journal*. Dr. Tarn is cofounder of the Telecommunications and Information Management program at Western Michigan University.

Mei-Yi Cheng received her MSC degree from the Department of Accounting and Information Technology, National Chung Cheng University, Taiwan. She is currently an auditor at HTC Corporation, Taiwan.