

SOX 404-compliant ERP System Internal Control Framework - The Preliminary Outcome

She-I Chang¹ and Derek Jan²

After the enactment of the Sarbanes-Oxley Act (SOX), the importance of related issues, such as internal controls and information security, has greatly increased. In the first stage of this research, the grounded theory methodology is adopted to explore the necessary internal controls in Information Technology (IT) systems. The control criteria are mapped out in the Criteria for Establishment of Internal Control framework. In the second stage, a case study will conduct to verify the feasibility of the first established framework. This paper eventually offers a 12-dimensional preliminary framework with a total of 37 control items to provide auditors with the capacity to perform effective audits by inspecting the essential internal control points in Enterprise Resource Planning (ERP) systems. Furthermore, it suggests that companies refer to this framework and consider the limitations of their own IT management in order to establish a robust IT management mechanism.

Keywords: Internal control framework; Enterprise Resource Planning; Sarbanes-Oxley Act (SOX)

Field of Research: Accounting Information Systems, IT Governance

1. Introduction

Due to the fact that Enterprise Resource Planning (ERP) systems is a popular and all-encompassing information system used by many organizations and the increased consideration of risks associated with IT, related information system security and the internal controls over these information systems have greatly increased (Dhillon, 2007; Walters, 2007). Evidence indicates that although computer abuse and information system security breaches may not necessarily result in serious problems, they do trigger huge losses (Richardson, 2003; Gordon et al., 2005). Generally, an attack on information causes theft of confidential data, financial fraud, an incapacitated web server, and corrupted operation data (Gordon et al., 2005). All of these influence the accuracy and reliability of financial data derived from the information system (Walters, 2007). Hence, understanding related risk management and control is critical to any organization implementing the ERP system.

For these reasons, the accuracy and reliability of the data within the ERP system is critical, especially if the financial data is sourced from system outputs. As a result, an

¹ Dr. She-I Chang, Department of Accounting and Information Technology, National Chung Cheng University, Taiwan. Email : actsic@ccu.edu.tw

² Mr. Derek Jan, KPMG, Taiwan. Email : derek.jan@gmail.com

increasing number of companies have begun to focus on the implementation of effective IT controls in their information environment while simultaneously providing the management and external auditor with a suitable framework to assess their IT control. In 1992, the Committee of the Sponsoring Organizations of the Treadway Commission (COSO) released a report entitled Internal Control-Integrated Framework (COSO 1992) in an attempt to illustrate a systematic framework for internal control. However, the report failed to list supplemental criteria to assist in the implantation and assessment of IT controls (O'Donnell and Rechtman, 2005; ISACA, 2007). One straightforward method to ensure normal ERP system operations, as well as compliance with SOX 404, is the implementation of a robust internal control framework that can easily be used by the management and the company auditors.

In light of the abovementioned conditions, this paper focuses on finding the preliminary framework for auditors to more effectively perform audits in ERP system. The research question provided in this paper is what are the key control items in building effective and robust internal control framework? And the research objectives of this paper are as follows: (1) Identification of necessary control-related considerations in information auditing cycles in an ERP system; and (2) Development of a preliminary internal control framework to be applied to information cycles in an ERP system. Section 2 of this paper is the literature review, which focuses on reviewing the relevant recent studies and discussions in the past. Section 3 illustrates the research method and design of this research. Section 4 discusses the process of building up the preliminary framework for the ERP internal controls and its outcome. Finally, section 5 provides suggestions to both managers and auditors in business fields as well as illustrates the study's limits and the scope for future work.

2. Literature Review

2.1 System Security and Internal Controls in the ERP system

In practice, the term "ERP" has been broadly used as a concept in the field of business management. According to Davenport (2000), an ERP system should be able to effectively provide real-time and integrated data to help a company operate and make decisions. This is especially true because the system integrates all of the major core levels of the operations of a company while tying everything closely with the system logic. Thus, an ERP system must be highly flexible and capable of catering to the overall strategies and operational guidelines of a company through the adjustment and modification of its system architecture. Due to these advantages, many software vendors have launched ERP software products in recent years (She and Thuraisingham, 2007).

An increasing number of firms have come to depend on the ERP system to deal with operational transactions. Therefore, information system security now must be emphasized, especially with regards to financial transactions. Walters (2007) indicates that many information system threats, including more severe forms such as unauthorized access and system vulnerabilities attacks, likely influence the accuracy and reliability of financial data derived from information systems. Information security acts to protect and control these information technology resources, consequently ensuring the accuracy and reliability of the information (Fox and Zonneveld, 2003). Van de Riet et al. (1998) suggests a number of security aspects associated with an ERP system, including security policy, user authentication, authorization, time restriction, log and trace, and database security.

Given that information security control can maintain both the reliability of the information system resource and the availability and integrity of financial data, it is also closely linked with internal controls. Following the enactment of SOX, company management teams are now required to take responsibility over their respective financial reports. The effectiveness of an internal control is indicated in SOX 404 (PCAOB, 2004; ITGI, 2005). Hence, information system security has become extremely relevant in SOX and must be fully considered by the management of a company (Byrum, 2003). Furthermore, if firms lack the proper level and type of information security, they fail to ensure the effectiveness of their internal controls and ultimately, the integrity of their financial data (Proctor and Vignaly, 2004).

2.2 Challenges of Audits and Inspections in the ERP System

The relationship between the financial reporting and auditing of companies can be described as follows: “accounting” is the process of gathering, consolidating, reporting, explaining, and analyzing financial information, whereas “audit” refers to the evidence and theories that prove the fairness or reasonability of the financial reporting as a whole (Bedard and Graham, 2002; Khurana and Raman, 2004). Accordingly, the use of generally accepted accounting principles as a benchmark for assessing the degree to which the financial statements of a company are fairly reported requires that audit processes follow specific standards in order to avoid inconsistencies (Arens et al., 2005). In certain situations, if an auditor issues an audit report that does not properly reflect the true financial state of a company (e.g., major inaccuracies in financial reports), audit risk is created.

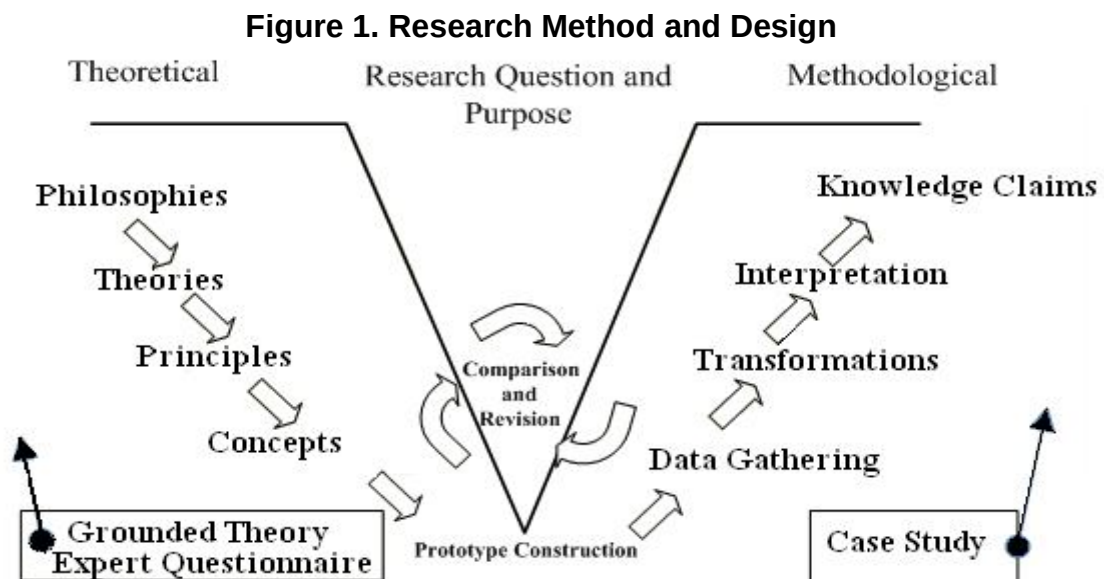
In traditional auditing processes, accountants mainly review the internal control framework of companies (i.e., management control and accounting control) (Khurana and Raman, 2004). Toward the attainment of sound audit quality, audits are now performed with the use of computer systems and relevant support tools, apart from the traditional audits that called for the manual inspection of forms and documents (Brazel, 2005; Li et al., 2007). The application of IT has resulted in the evolution of auditing methods. Nevertheless, choosing between IT-related methods and the traditional audit approach is heavily based on considerations related to the costs, benefits, and efficiency of audits, the compatibility of hardware facilities and software programs, the possibility of reviews on audit tracks and relevant documents, and the computer audit abilities of auditors and inspectors (Wu, 2005).

The introduction of a new information system in a company may bring about a risk different from those initially associated with the legacy framework. In fact, risks that accompany new framework operations may not be the same as those of the original system (O’Leary, 2000). In terms of the ERP system, the reengineering of business process, and organizational changes brought about by the introduction of the new system may also lead to changes in the control requirements of a company (Chang and Gable, 2002). In general, problems frequently associated with the ERP system are contained. These include those related to business interruption, process interdependency, network security, database security, application security, and overall internal controls (Hunton et al., 2004). Therefore, in relation to the ERP system, many key aspects of the risk control environment must be taken into account (Sally and Arnold, 2002). Glover et al. (1999) likewise suggest that internal auditors should consider the relevant risks and controls required for system planning based on their knowledge of risk management and the internal risks present in the company

during the introduction of the ERP system. To effectively perform internal controls over the ERP system, auditors and inspectors should first understand the basic architecture of the ERP system (AICPA, 2001; Calabro, 2004). Altogether, under the comprehensive application of the IT environment, auditors should equip themselves with relevant computer knowledge and skills, otherwise, the audit work on the information system of the ERP system will present many obstacles and challenges (Steven, 1999; Cerullo, 2000; Hunton et al., 2004).

3. Research Method and Design

In an attempt to develop an internal control framework for the ERP system based on the previously mentioned frameworks, such as the COSO Framework of 1992, this study employed the grounded theory. This theory is considered an important methodology in qualitative research because it analyzes, consolidates, and generalizes complex concepts. Glaser and Strauss (1967) indicate that the constructs of the grounded theory research method require a theoretical saturation, connoting that researchers ought to continue their sampling until no new or relevant data appear in any domain. The literature also stresses that the development of each domain be widespread, and that only when every part is tightly interconnected and both the processes and variances are fully apparent can the sampling cease. In addition, Strauss (1987) suggests that the final part of a research study may depend on external conditions even if theories have already been constructed. External conditions mainly include time, financial support, personal interest, and the knowledge domains of the researchers. The research method and design of this paper are illustrated in Figure 1.



4. The Preliminary Framework for the ERP Internal Controls

4.1 Data Collection and Analysis

This paper gathered relevant literature from the following sources: (1) Information cycle controls for the internal use of companies. The data gathered is expected to be within the scope of internal use for companies and can thus be compiled with the current internal control bylaws of the corporate information system; (2) Information

security organization bylaws. This paper mainly refers to the regulations and criteria of COBIT and BS7799 and covers all of the systems of information; both are important references since they have been adopted by many companies (Tuttle and Vandervelde, 2007); and (3) Other literature.

The Science Direct database was used to search for academic literature. The main criteria are as follows: (1) Key words or abstracts must have the words “Information Security” or “Internal Control”; (2) The classification of literature must be related to information and studies must have been published within the past five years.

Based on the above criteria, this paper collected conceptualized results from 30 relevant publications. The collected results are shown in Appendix 1. This paper also performed a detailed analysis to present a complete and consistent list of internal control items for information cycles. The preliminary model was constructed using the grounded theory methodology with the whole process roughly divided into three steps: (1) open coding, (2) axial coding, and (3) selective coding.

Open coding

At this stage, this paper performed coding for the contents mentioned in the literature that satisfy the criteria mentioned above. As defined in the research purpose, “Construction of the Internal Control for the Information Cycle – The ERP System as an Example,” the research study allows for section extraction and codes these sections if they are identified as paragraphs relevant to the internal controls of the information operations or if they obviously indicate components of information control of the information operations. Coding was conducted in order to classify the literature from A to C. For example, “W Company – Computerized Information System ICE” includes a section that deals with internal regulations. More specifically, this section mentions that, “coming online requires test reports or passing of tests.” This implies that this description can be conceptualized and coded into three factors (i.e., A216, whether or not there are test documents; A217, whether or not there are independent test environments; or A218, whether or not they have been verified by users).

Axial coding

Axial coding is usually conducted after the completion of open coding. The purpose of this stage is to recompose the distributed data into new methods to make the classifications and sub-classifications become related to one another. Thus, the more accurate and complex interpretations could be established as certain phenomena (Strauss, 1987). As such, concepts were translated into domains; 66 domains were established as internal control key issues based on the 670 concepts determined in the open coding process. To comply with the regulations and standards and to achieve the research goals, this paper referred to the guidelines for control operations in the Criteria for Establishment of Internal Control Frameworks by Public Companies as defined by the Securities and Futures Bureau. The fundamental dimensions set for this paper are as follows:

- Definition of functions and responsibilities of the data processing department;
- System development and control over program modifications;
- Control over the compilation of system documents;
- Access control of programs and data;

Chang & Jan

- Control of data inputs and outputs;
- Control of data processing;
- Security control of files and equipment;
- Control over the procurement, and use and maintenance of hardware and system software;
- System recovery plans/systems and control of testing programs;
- Control of information/communication security inspections;
- Independent information audit units; and
- Control over the processes of information disclosures on the websites assigned by the Securities and Futures Bureau.

Selective coding

According to the grounded theory, axial coding consolidates complex data and is the foundation for selective coding. Selective coding is conducted to systematically explain a selected core category, verify the relationship of the main classifications and other classifications, and fill the gap for the supplements or developments required for individual classifications (Strauss, 1987).

In terms of the key issues of the internal controls over information cycles, and the analysis of relevant literature, this research study identified 66 key factors that influence the internal control of information systems. In the process of selective coding, the results of the previous axial coding integrated items were re-classified as single key factors. For example, the factors, “whether there are anti-virus measures,” and “whether there are firewalls,” were merged into, “whether there are security and protection measures.” Subsequently, 51 key factors emerged.

4.2 Expert Questionnaires

Upon the completion of the construction of the preliminary internal control items based on the grounded theory, this paper adopted the methodology and validation process developed by Lawshe (1975). The adoption of this methodology and validation process enabled the collection of ideas and opinions from experts with extensive experience in the establishment, maintenance, and auditing processes of the ERP system. Expert questionnaires were issued in the process and the basic information of experts is listed in Table 1. All the measurement dimensions and item indicators were screened in order to extract those suitable for and essential to the ERP system. In fact, this approach enhanced the practice and experience earlier discussed in this paper. The applications of both theories and practices are expected to effectively increase the validity, extent, and practicality of this paper, thus achieving the research purpose of constructing the internal control of the information system in an ERP system.

Table 1. Basic Information of Experts

Group	Type	No. of People	Positions	Average years of service
Experts within Companies	Audit	6	Senior Auditors * 4	14
			Audit Specialists * 2	
	IT	5	Manager, MIS * 1	11
			Assistant Manager, MIS * 3	
			Deputy Project Manager, MIS * 1	
Experts outside Companies	Professional firms	5	Computer Audit, Manager * 1	6
			Computer Audit, Assistant Manager * 1	
			Computer Audit, Assistant VP * 1	
			Audit, Manager * 1	
			Audit, Director * 1	
	ERP consultants	2	Consultants * 2	7

The expert questionnaire used by this paper measured the opinions of respondents based on an ordinal scale of 5, from “very important (5),” “important (4),” “ordinary (3),” “unimportant (2),” to “very unimportant (1).” Each dimension was made semi-open so that the responding experts could provide relevant feedback on the key items related to internal control in the ERP system as proposed by this paper.

A total of 18 experts responded to the questionnaires. According to the methodology and validation process proposed by Lawshe (1975), the Content Validity Ratio (CVR) can be calculated as $CVR = (n - N/2) / (N/2)$. Herein, “n” represents the number of times that experts categorized the items as either “very important” or “important,” while “N” represents the total number of experts. The CVR value should be greater than 0.43 to meet the targeted requirements. To ensure that the control items constructed by this study remain important and feasible for the majority of the companies, this paper required that a CVR ratio be greater than 0.60 before a control item could be adopted. Appendix 2 summarizes the expert questionnaire results, including the statistics from the expert questionnaires and the calculation of the CVR.

As mentioned earlier, the research referred to the grounded theory in its literature review, and identified 51 key items for the internal control of information systems. Upon calculation and comparison of the CVR values gathered from the expert questionnaires, 14 items considered unimportant were deleted; the remaining 37 control items were generalized and consolidated. This paper further modified its preliminary internal control items by referring to the suggestions provided by the expert respondents. Figure 2, the preliminary framework for the ERP internal control shows the amendments offered based on the feedback.

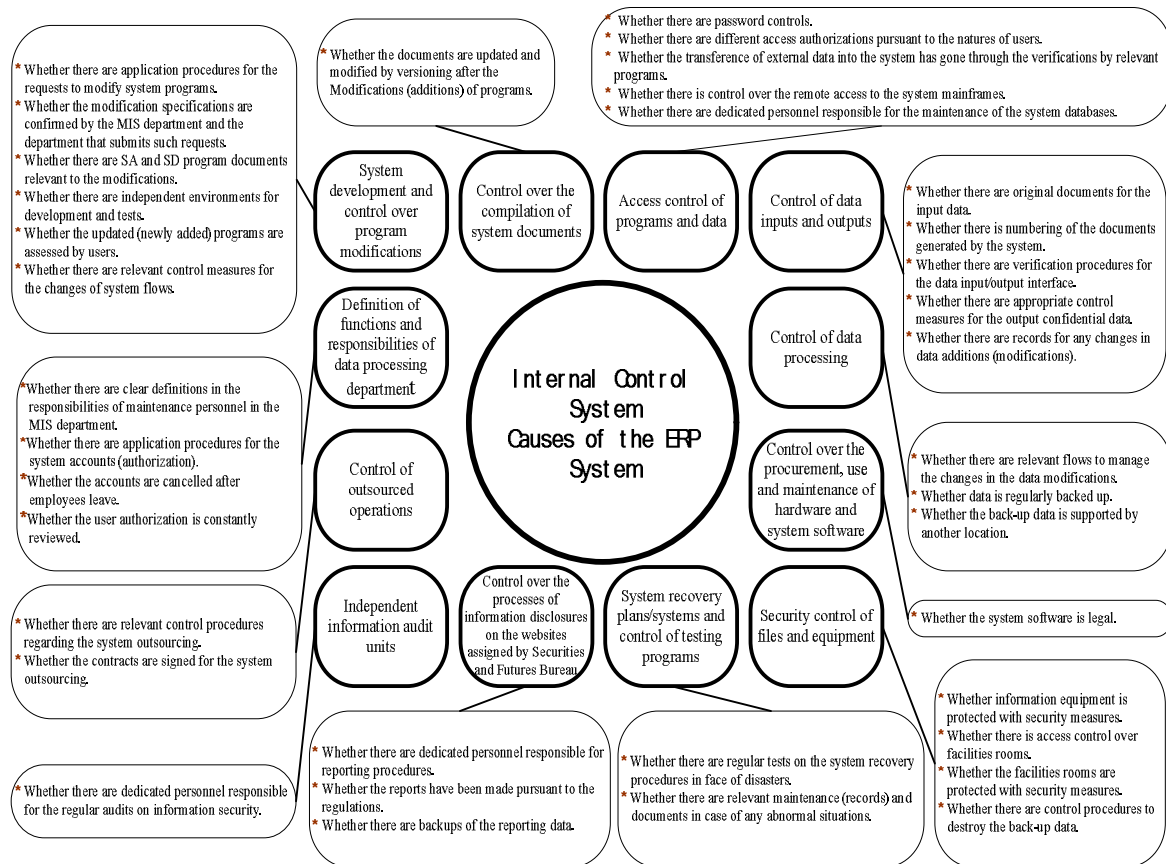


Figure 2. The Preliminary Framework for the ERP Internal Controls

5. Conclusions and Limitations

Given that the ERP system is widely employed in many organizations, relevant information on security and internal controls must be continuously stressed. Improper management control procedures in a computer environment may result in huge financial losses and financial reporting errors for a company. This study has developed a preliminary ERP internal control framework to assist stakeholders in verifying the effectiveness of their own internal control mechanisms. For managers, this framework allows them to identify weaknesses in the internal controls of their company which will in turn help them reinforce their control mechanisms to comply with the set regulations. In addition, the framework can provide auditors with a guide to confirm and report on management's assessment of internal controls in order to mitigate their audit risk. All the research aspects, such as research framework, data collection and analysis, questionnaire design, and conduct of the questionnaire, are comprehensive. However, the research still has its limitations. Due to the differences in scale and types of industries, each enterprise has different demands on the aspect of ERP internal controls. Though the results in this research might not suit for each enterprise, the preliminary framework established in this research can help enterprises examine whether their own IT management mechanisms are well-developed enough.

References

- American Institute of Certified Public Accountants (AICPA), 2001, *The effect of information technology on the auditors' consideration of internal control in a financial statement audit*, SAS No. 94, AICPA, New York.
- Arens, A. A., R. J. Elder, and M. S. Beasley. 2005, *Auditing and assurance services: Auditing: an integrated approach*, Prentice Hall, New Jersey.
- Bedard, J. C., and L. E. Graham. 2002. "The effects of decision aid orientation on risk factor identification and audit test planning", *Auditing*, vol. 21, no. 2, pp. 39-65.
- Brazel, J. F. 2005. "A measure of perceived auditor ERP systems expertise: Development, assessment, and uses", *Managerial Auditing Journal*, vol. 20, no. 6, pp. 619-632.
- Byrum S. 2003. "The impact of Sarbanes-Oxley Act on IT Security", *SANS Institute*. Available at: <http://www.sans.org/rr/whitepapers/casestudies/1344.php>.
- Calabro, L. 2004. "Looking under the hood", *CFO*, vol. 20, no. 6, pp. 97-98.
- Cerullo, M. J. 2000. "The internal auditor's role in developing and implementing enterprise resource planning systems", *Internal Auditing*, vol.15, no. 3, pp. 25-34.
- Chang, S. I. and G. G. Gable. 2002. "A comparative analysis of major ERP lifecycle implementation, management and support issues in Queensland government", *Journal of Global Information Management*, vol. 10, no. 3, pp. 36-54.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 1992, *Internal control - integrated framework*. AICPA, NY.
- Davenport, T. H. 2000, *Mission critical: Realizing the promise of enterprise systems*, Harvard Business School Press, Boston.
- Dhillon, G. 2007, *Principles of information system security: Text and cases*, John Wiley and Sons, NJ.
- Fox, C., and P. C. Zonneveld. 2003, *IT control objectives for Sarbanes-Oxley: The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting*, IT Governance Institute, IL.
- Glaser, B., and A. Strauss. 1967, *The discovery of grounded theory*, Aldine, Chicago.
- Glover, S., D. Prawitt, and M. Rommy. 1999. "Implementing ERP", *Internal Auditor*, vol. 56, no. 1, pp. 40-47.
- Gordon, L. A., M. P. Leob, W. Lucyshyn, and R. Richardson. 2005. "CSI/FBI Computer Crime and Security Survey", *Computer Security Institute*. Available at: www.qocsi.com.
- Hunton, J. E., A. M. Wright, and S. Wright, 2004. "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?" *Journal of Information Systems*, vol. 18, no. 2, pp. 7-28.
- Information System Audit and Control Association (ISACA), 2007, *IS standards, guidelines and procedures for auditing and control professionals*, ISACA, IL.
- IT Governance Institute (ITGI). 2005, *Control objectives, management guidelines, maturity models in CobiT 4.0*, IT Governance Institute, IL.
- Khurana, I. K., and K. K. Raman. 2004. "Litigation risk and the financial reporting credibility of big 4 versus non-big 4 audits: Evidence from Anglo-American countries", *Accounting Review*, vol. 79, no. 2, pp. 473-495.
- Lawshe, C. H. 1975. "A quantitative approach to content validity", *Personnel Psychology*, vol. 28, no. 4, pp. 563-575.
- Li, S. H., S. M. Huang, , and Y. C. Lin. 2007. "Developing a continuous auditing assistance system based on information process models", *Journal of Computer Information Systems*, vol. 48, no. 1, pp. 2-13.

Chang & Jan

- O'Donnell, J. B., and Rechtman. 2005. "Navigating the standards for information technology controls", *The CPA Journal*, vol. 75, no. 7, pp. 64-69.
- O'Leary, D. 2000, *Enterprise resource planning systems: Systems, life cycle, electronic commerce, and risk*, Cambridge University Press, Cambridge.
- Proctor, P., and J. Viganly. 2004, The security implications of Sarbanes-Oxley, *Symantec Enterprise Solutions Webcast*. Available at: www.symantec.com/press/2004/n040218c.html.
- Public Company Accounting Oversight Board (PCAOB). 2004, *An audit of internal control over financial reporting performed in conjunction with an audit of financial statement*. Auditing Standard No. 2. PCAOB, DC.
- Richardson, R. 2003, CSI/FBI Computer Crime and Security Survey. Available at: www.qocsi.com.
- Sally, W., and M. W. Arnold. 2002. "Information system assurance for enterprise resource planning system: Unique risk considerations", *Journal of Information Systems*, vol. 16, no. 1, pp. 99-113.
- She, W. and B. Thurasingham. 2007. "Security for enterprise resource planning systems", *Information Systems Security*, vol.16, no. 3, pp. 152-163.
- Steven, M.G. 1999. "Implementing ERP", *The Internal Auditor*, vol. 56, no. 1, pp. 40-46.
- Strauss, A. 1987, *Qualitative analysis for social scientists*, Cambridge University Press, Cambridge.
- Tuttle, B., and S. D. Vandervelde. 2007. "An empirical examination of CobiT as an internal control framework for information technology", *International Journal of Accounting Information Systems*, vol. 8, no. 4, pp. 240-263.
- Van De Riet, R., W. Janssen, and P. De Gruijter. 1998, *Security moving from database systems*. Database and Expert System Applications Proceedings.
- Walters, L. M. 2007. "A draft of an information systems security and control course", *Journal of Information Systems*, vol. 21, no. 1, pp. 123-148.
- Wu, C.P. 2005, *Accounting and financial information system*, Chi Sheng, Taipei.

Chang & Jan

Appendix 1. Related Literature of IT Internal Control

No	Author	Year	Literature Title	Literature Source
1	A company	2006	Computerized Process- Internal Control	A company
2	B company	2006	Computerized Process- Operation	B company
3	C company	2006	Computerized Process- Internal Control	C company
4	British Standards Institution	2004	BS 7799	British Standards Institution (BSI)
5	IT governance Institute	2005	Control objectives for information and related technology (COBIT 4.0)	Information Systems Audit and Control Association
6	Cerullo and Cerullo	2004	Business continuity planning: A comprehensive approach.	Information Systems Management
7	Chau	2006	Application security – it all starts from here.	Computer Fraud & Security
8	Coe	2005	Trust services: A better way to evaluate IT controls.	Journal of Accountancy
9	Da Veiga and Eloff	2007	An information security governance framework.	Information Systems Management
10	Eloff and Eloff	2005	Information security architecture.	Computer Fraud & Security
11	Flowerday and Von Solms	2005	Continuous auditing: verifying information integrity and providing assurances for financial reports.	Computer Fraud & Security
12	Gorge	2005	USB & other portable storage device usage: Be aware of the risks to your corporate data in order to take pre-emptive and/or corrective action.	Computer Fraud & Security
13	Hunter	2005	Card Systems: four million hack – under the spotlight.	Computer Fraud & Security
14	Jones	2006	The convergence of physical and electronic security.	Computer Fraud & Security
15	Marks	2004	The more things change...	Internal Auditor
16	Myler and Broadbent	2006	ISO 17799: Standard for security.	Information Management Journal
17	Saint-Germain	2005	Information security management best practice based on ISO/IEC 17799.	Information Management Journal
18	Stephenson	2005	Incident analysis and recovery.	Computer Fraud & Security
19	Stephenson	2006	Ensuring consistent security implementation within a distributed and federated environment.	Computer Fraud & Security
20	Stewart	2004	On risk: perception and direction.	Computers & Security
21	Thomson and Von Solms	2006	Towards an information security competence maturity model.	Computer Fraud & Security
22	Tyson and Bean	2005	System access hotspots: Are auditors ignoring danger?	Journal of Corporation Accounting & Finance
23	Volonino and Gessner	2004	Holistic compliance with Sarbanes- Oxley.	Communication of AIS
24	Von Solms	2005	Information security governance – compliance management vs. operational management.	Computers & Security
25	Wallace et al.	2004	Understanding software project risk: a cluster analysis.	Information & Management
26	Williams	2003	Performing a successful Unix audit.	Computer Fraud & Security
27	Flowerday and Von Solms	2005	Real time information integrity= system integrity +data integrity+ continuous assurances	Computers & Security
28	Walters	2007	A draft of an information systems security and control course	Journal of Information Systems
29	She and Thuraisingham	2007	Security for enterprise resource planning systems	Information System Security
30	Wilson	2005	Risk control: A technical view.	Computer Fraud & Security
NO.1-3 are classified as A (information cycle control for the internal use of companies) NO.4-5 are classified as B (Information Security organization bylaws) NO.6-30 are classified as C (academic literature)				

Chang & Jan

Appendix 2. Expert Questionnaire Analysis

Dimension	No.	Control Items	Types						Groups		
			CVR, CPA firm	CVR, MIS	CVR, Audit	CVR, ERP consultant	CVR, all experts	Screen results	CVR, external experts	CVR, internal experts	Perception difference between groups
Definition of functions and responsibilities of data processing department	1	Whether there are clear definitions of the responsibilities of maintenance personnel in the MIS department.	1.00	0.60	1.00	1.00	0.89	Yes	1.00	0.82	No
	2	Whether there are application procedures for the system accounts (authorization).	1.00	1.00	1.00	1.00	1.00	Yes	1.00	1.00	No
	3	Whether the accounts are cancelled after employees leave.	0.60	0.60	1.00	1.00	0.78	Yes	0.71	0.82	No
	4	Whether user authorization is constantly reviewed.	1.00	0.20	1.00	0.00	0.67	Yes	0.71	0.64	No
	5	Whether there is a dedicated team responsible for the maintenance of the hardware and software of the system.	-0.20	1.00	0.67	1.00	0.56	No	0.14	0.82	Yes
System development and control over program modifications	1	Whether there are application procedures for the requests to modify system programs.	1.00	1.00	1.00	1.00	1.00	Yes	1.00	1.00	No
	2	Whether the modification specifications are confirmed by the MIS department and the department that submits such requests.	1.00	1.00	0.67	1.00	0.89	Yes	1.00	0.82	No
	3	Whether there are SA and SD program documents relevant to the modifications.	0.60	1.00	1.00	0.00	0.78	Yes	0.43	1.00	Yes
	4	Whether there are independent environments for development and tests.	1.00	1.00	1.00	1.00	1.00	Yes	1.00	1.00	No
	5	Whether there are relevant test documents and records on program developments.	0.20	0.60	0.67	0.00	0.44	No	0.14	0.64	Yes
	6	Whether the updated (newly added) programs are assessed by users.	1.00	1.00	1.00	1.00	1.00	Yes	1.00	1.00	No
	7	Whether there are relevant control measures for the changes of system flows.	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
Control over the compilation of system documents	1	Whether there are coding management on the documents in relation to program modifications (updates).	0.60	0.60	0.00	0.00	0.33	No	0.43	0.27	No
	2	Whether the documents are updated and modified by versioning after the modifications (additions) of programs.	1.00	1.00	1.00	0.00	0.89	Yes	0.71	1.00	No
	3	Whether there are dedicated personnel safeguarding the documents in relation to the systems.	-0.20	1.00	0.67	-1.00	0.33	No	-0.43	0.82	Yes
	4	Whether only certain personnel can access (modify) the documents in relation to the system programs or the original library.	0.20	0.60	1.00	0.00	0.56	No	0.14	0.82	Yes
Access control of programs and data	1	Whether there are password controls.	1.00	1.00	1.00	1.00	1.00	Yes	1.00	1.00	No
	2	Whether there are different access authorizations pursuant	1.00	1.00	1.00	1.00	1.00	Yes	1.00	1.00	No

Chang & Jan

			Types						Groups		
Dimension	No.	Control Items	CVR, CPA firm	CVR, MIS	CVR, Audit	CVR, ERP consultant	CVR, all experts	Screen results	CVR, external experts	CVR, internal experts	Perception difference between groups
		to the natures of users.									
	3	Whether the transference of external data into the system has undergone verification by relevant programs.	1.00	1.00	1.00	0.00	0.89	Yes	0.71	1.00	No
	4	Whether there is control over the remote access to the system mainframes.	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
	5	Whether there are dedicated personnel responsible for the maintenance of the system databases.	1.00	1.00	0.67	1.00	0.89	Yes	1.00	0.82	No
Control of data inputs and outputs	1	Whether there are original documents for the input data.	1.00	0.60	1.00	0.00	0.78	Yes	0.71	0.82	No
	2	Whether there is numbering of the documents generated by the system.	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
	3	Whether there are verification procedures for the data input/output interface.	0.60	0.60	1.00	0.00	0.67	Yes	0.43	0.82	Yes
	4	Whether there are appropriate control measures for the output confidential data.	-0.20	1.00	1.00	1.00	0.67	Yes	0.14	1.00	Yes
	5	Whether there are records for any changes in data additions (modifications).	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
Control of data processing	1	Whether there are relevant flows to manage the changes in the data modification.	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
	2	Whether data is regularly backed up.	0.20	1.00	1.00	1.00	0.78	Yes	0.43	1.00	Yes
	3	Whether the backup data is supported by another location.	0.20	0.60	1.00	1.00	0.67	Yes	0.43	0.82	Yes
Security control of files and equipment	1	Whether information equipment is listed and managed.	-0.60	0.60	0.67	0.00	0.22	No	-0.43	0.64	Yes
	2	Whether information equipment is protected with security measures.	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
	3	Whether there is access control over facility rooms.	0.20	1.00	1.00	1.00	0.78	Yes	0.43	1.00	Yes
	4	Whether the facility rooms are protected with security measures.	-0.20	1.00	1.00	1.00	0.67	Yes	0.14	1.00	Yes
	5	Whether there are control procedures to destroy the backup data.	-0.20	0.60	1.00	1.00	0.56	Yes	0.14	0.82	Yes
Control over the procurement, use, and maintenance of hardware and system software	1	Whether there are dedicated personnel responsible for the maintenance of software updates.	0.20	1.00	0.33	0.00	0.44	No	0.14	0.64	Yes
	2	Whether there are regular inspections on hardware daily logs.	-0.20	1.00	0.67	1.00	0.56	No	0.14	0.82	Yes
	3	Whether the software and hardware are regularly maintained.	-0.20	1.00	0.33	1.00	0.44	No	0.14	0.64	Yes
	4	Whether there are records to note the maintenance and	-0.60	1.00	0.67	1.00	0.44	No	-0.14	0.82	Yes

Chang & Jan

			Types						Groups		
Dimension	No.	Control Items	CVR, CPA firm	CVR, MIS	CVR, Audit	CVR, ERP consultant	CVR, all experts	Screen results	CVR, external experts	CVR, internal experts	Perception difference between groups
		changes of hardware and software.									
	5	Whether the system software is legal.	0.20	1.00	1.00	1.00	0.78	Yes	0.43	1.00	Yes
System recovery plans/systems and control of testing programs	1	Whether there are regular tests on the system recovery procedures in face of disasters.	0.20	1.00	0.67	1.00	0.67	Yes	0.43	0.82	Yes
	2	Whether there are procedures to report disasters.	-0.60	1.00	0.67	1.00	0.44	No	-0.14	0.82	Yes
	3	Whether there are relevant maintenance (records) and documents in case of any abnormal situations.	0.20	1.00	1.00	0.00	0.67	Yes	0.14	1.00	Yes
Control over the processes of information disclosures on the websites assigned by Securities and Futures Bureau	1	Whether there are dedicated personnel responsible for reporting procedures.	0.20	1.00	1.00	1.00	0.78	Yes	0.43	1.00	Yes
	2	Whether the reports have been made pursuant to the regulations.	0.60	1.00	1.00	1.00	0.89	Yes	0.71	1.00	No
	3	Whether there are backups of the reporting data.	0.20	1.00	0.67	1.00	0.67	Yes	0.43	0.82	Yes
Independent information audit units	1	Whether there is system security planning.	0.20	1.00	0.67	0.00	0.56	No	0.14	0.82	Yes
	2	Whether there are dedicated personnel responsible for the regular audits on information security.	0.60	0.60	1.00	1.00	0.78	Yes	0.71	0.82	No
	3	Whether there are promotions and training programs targeted at internal staff on information security.	-0.20	0.60	0.67	0.00	0.33	No	-0.14	0.64	Yes
Control of outsourced operations	1	Whether there are relevant control procedures regarding the system outsourcing.	0.60	0.60	0.67	1.00	0.67	Yes	0.71	0.64	No
	2	Whether there are evaluations on the system outsourcing.	0.20	0.60	0.67	1.00	0.56	No	0.43	0.64	Yes
	3	Whether the contracts are signed for the system outsourcing.	0.60	0.60	1.00	1.00	0.78	Yes	0.71	0.82	No