Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

AN EMPIRICAL STUDY OF THE RELATIONSHIP BETWEEN ITGC, COMPLIANCE, AND IT-RELATED RISK IN CHINA

WING HAN BRENDA CHAN
UNIVERSITY OF MACAU
brendac@umac.mo

KIN-MENG SAM
UNIVERSITY OF MACAU
tonysam@umac.mo

DAN LIU
peperannliu@hotmail.com

ABSTRACT

This research proposes a deductive-nomological model studying whether the mitigation of IT-related risks and regulatory compliance can be achieved through information technology general controls (ITGC). A quantitative survey was conducted with enterprises in China. Research findings suggest that effective ITGC help organizations meet regulatory requirements. Sound regulatory compliance helps promote a stronger IT control environment. Yet many Chinese enterprises with ITGC and complying with regulations show weak intention to the mitigation of IT-related risks. Without a risk-based internal control system, compliance itself does not contribute to the goal of risk mitigation. Chinese enterprises need to enhance their IT control ability and to learn to be more risk-oriented in order to cope with ever increasing IT-related risks.

Keywords Information Technology General Controls (ITGC); IT Control; IT-related Risks; Compliance; Committee of Sponsoring Organizations of the Treadway Commission (COSO).

INTRODUCTION

Organizations utilize information technology (IT) to establish and maintain new governance processes with improved operational efficiency [22, 23, 29]. Yet IT can also expose organizations to an increasing set of risks and higher business impact [35, 78]. Risk is the likelihood of threat exploiting the vulnerability and exerting adverse impact on organizations [9, 20]. IT operational risks may impair IT assets and data quality in terms of integrity, confidentiality, and availability. Information security, privacy risk, threat of business disruption due to disasters and denial-of-service attacks are just a few examples of business risks closely related to IT nowadays. Organizations are confronted with emerging new business risks under the information environment, known as IT-related risk, such as application vulnerabilities, malware, configuration mistakes, asset theft, data leakages, and reputation damage [9, 24].

Internal controls, policies, and procedures established to achieve organizational objectives serve as important mechanisms for risk mitigation [45]. There are examples showing that IT-related risks may sabotage an organization's objectives if related technology controls and process controls are inadequate [71]. Based on the

2015 Global State of Information Security Survey conducted by PricewaterhouseCoopers (PwC), the frequency and costs of security incidents are on a rising trend, yet few organizations have updated critical information security processes and technologies. The average estimated financial loss attributed to cybersecurity incidents alone in 2014 was $2.7 million, 34% higher than 2013 [65]. However, IT-related risks cannot be easily detected with traditional controls [2, 35, 80].

As a single security breach or IT incident in an organization may cause serious impacts not only to the organization itself but also to the market, regulators have a high concern on the security of the information technology and systems of businesses and the integrity of data and processes that the systems support. In the U.S., internal control systems include the Sarbanes-Oxley Act (SOX), the Committee of Sponsoring Organizations of the Treadway Commission (COSO) frameworks, the Securities and Exchange Commission (SEC), and the Public Company Accounting Oversight Board (PCAOB). These systems have all considered the impacts of IT to the economy. In Japan, the Financial Reporting Internal Control Evaluation and Auditing Standards recognizes IT as an element of the internal control framework. In China, the recognition of the impact of IT controls is rising, though mainly restricted to the COSO reporting before 2012. The Basic Internal Control Norms for Enterprises (hereinafter referred to as the Basic Norms) and the Enterprise Internal Control Guidelines (hereinafter referred to as the Guideline) were introduced for the first time as authority guidelines for the internal control development of Chinese organizations. No. 18 of the Guidelines specifically addresses enterprise internal control over information systems (IS). All these show the trend that IT controls are one of the core elements in the internal control system of enterprises worldwide and the compliance with these regulations is necessary.

IT controls comprise of two categories, IT general controls (ITGC) and IT application controls (ITAC) [16]. ITAC are unique in different business environment and thus a generalized study on it poses great challenge. On the other hand, ITGC lay the foundation for reliability on information generated from practically all systems [59]. ITGC's establishment in organization is usually accompanied by compliance requirements (e.g., the SOX) and the complex IS environment of the business. ITGC also provide the foundation for ITAC as well as assurance to the operations of IS [59]. PCAOB Auditing Standard No. 2 acknowledges the unique nature of IT controls and allows a benchmarking auditing approach when ITGC are assessed [61]. ITGC should be perceived not only as IS management or regulatory compliance but also as an integral part of enterprise risk strategy.

This research intends to analyze the relationship between ITGC, mitigation of IT-related risk, and regulatory compliance. Organizations address risks with effective internal controls that support strategic, operational, and compliance objectives [26]. Though compliance, risk management, and internal controls are often described as closely interrelated [68, 79], little research has been devoted to these areas. In particular, it is interesting to find out how Chinese enterprises are doing as China has achieved the second largest economy in the world in 2014 and 2015 according to the International Monetary Fund. China's agenda for the G20, the International Monetary Fund, the international trade and investment policies and including those aimed at the internationalization of the renminbi (RMB) require Chinese enterprises reaching international standards of IT management and risk management. As such, this study aims at confirming the contributive role of ITGC to organizations in China from an enterprise IT-risk management perspective. Most academic studies on IT controls adopted case-study methods. This study suggests an empirical quantitative research to identify more insight and to answer the following research questions:

1. Does ITGC implementation in Chinese enterprises contribute to the mitigation of IT-related risk?
2. What role does compliance play in the relationship between ITGC and mitigation of IT-related risk?

LITERATURE REVIEW

IT-Related Risks and Management

Risk management aims to minimize loss and to create the best value for security purpose by identifying, measuring, and controlling uncertain events. Businesses are heavily dependent on IS for the fulfillment of operations and transactions. But what trailing behind can be negative uncertainties. Reynolds [67] described IT-related risks as spanning a broader spectrum and including risks associated with failure in IT systems and processes to comply with government regulations (e.g., SOX), security breach, attacks by hackers, denial-of-service and business disruption, and privacy issues relating to personal data leakage. Frost and Sullivan [24] raised the concern on the wide application of mobile devices, mobility, social media, and cloud computing as they pose risks such as exposing confidential information to unauthorized sources, data leaks, weak system controls, disruptions to operations of data center, all of which affect

organizations' operations and reputation. Organizations are confronting with emerging IT-related risks [9], and their dependence on IS and IT platforms bring along IT-based business risks, leaving standard business risks still in place [72]. The management and mitigation of IT-related risks are essential [33]. Organizations need to implement well-designed internal controls apart from taking full management accountability in order to reduce the exposure to and the potential impact of IT-related risks [67]. This is consistent with the findings in the IT Risk Management Report from Symantec, one of the world's most famous company for security and software making, which stated that well-designed controls together with best practice processes constitute effective IT risk management. The report shows that fewer IT incidents happen in organizations which have adopted not only good technology controls but also effective process controls [73, 74].

Internal Controls and IT Controls

IT controls refer to the management, operation, and technical safeguards or counter-measures prescribed for an IS to protect the confidentiality, integrity, and availability of the system and its information [58]. IT controls are very often embraced within the systems of internal controls which bring about protection to IT resources and enhancing the integrity, accuracy, and reliability of financial data [19, 27]. Internal controls instantly detect and alert enterprises the presence of risks and carry out routine and comprehensive assessment on the nature and extent of exposed risks [45]. A strong system of internal controls is essential to enterprise risk management (ERM) because it helps to mitigate the increasing security and privacy risks leading to violation of privacy laws [15]. COSO-ERM intends to enhance risk management and to improve the internal control process. To address the changing business environment with increasing relevance to IT, COSO updated its Internal Control-Integrated Framework in 2013 by integrating IT into internal control concepts [41]. Another internal control framework within IT context is COBIT which links risk management with business processes and internal controls. Lainhart [46] commented that the widely accepted COBIT framework provides best practice in the management of IT controls.

IT Governance Institute (ITGI) suggested the inclusion of the IT dimension when defining, planning, and implementing internal control as it is playing an important role in achieving company objectives [39]. Flowerday and Von Solms [22] studied IT control's contribution toward information quality through maintaining a secure, integrated, and reliable system and database. Li et al. [48] identified a positive relationship between the strength of IT controls in the management of IS and the reliability of the information produced. If organizations are weak in IT controls, they are likely to have more non-IT related weakness and misstatements [44]. An effective IT control environment would indicate fewer IT-related risks with less negative impact and lower possibility of happening [63]. These studies provided evidence that ineffective IT controls can cause pervasive negative impacts on organization's control environment and risk assessment.

ITGC Processes

IT controls are designed to target at the IT infrastructure including policies, processes, systems, applications, and information of an organization [27]. There are two categories of IT controls: (1) information technology application controls (ITAC) and (2) information technology general controls (ITGC) [16, 27]. ITGC deal with IT processes and services, including systems development, change management, and the safety and execution of operations. ITGC processes contribute to business value and help improving firm performance [11]. ITGC also affect the consistency and effectiveness of business system applications [35]. The Guide to the Assessment of IT Risk (GAIT) presents that when IT control objectives are achieved through IT control processes, IT-related risks are mitigated. GAIT describes relationships between IT risks and financial statements, key controls within business processes, automated controls and other critical IT functionality, and key controls within ITGC. Developing an understanding in the IT control environment and its related controls and processes are crucial to risk assessment [7]. According to the Controls Over Information Technology Systems of the IT Governance Institute, IT control processes include the following [40]:

- IT control environment: includes IT governance, monitoring and reporting. IT governance ensures IT adds value and IT risks are mitigated. Monitoring and reporting ensure IT is aligned with the business. IT governance process covers the IS strategic plan, the IT risk management process, compliance and regulatory management, IT policies, procedures and standards.
- Computer operations: include controls over definition, acquisition, installation, configuration, integration, and maintenance of the IT infrastructure. Ongoing controls

over daily operations address the delivery of information services.

- Access to programs and data: Access control provides assurance against inappropriate access, unauthorized use of system, and intrusion of malicious software.
- Program development: includes the acquisition and implementation of new applications. A proper system development and quality assurance methodology supports identification of automated solutions, system design and implementation, documentation requirements, testing, approvals, project management and oversight requirements, and project risk assessment.
- Program change: appropriate controls over changes ensure that they are made properly. Controls involve required authorization of change requests, review of changes, approvals, documentation, testing and assessment of changes on other IT components and implementation protocols.

Regulatory Compliance and the Impact of SOX Act

Organizations have compliance obligations to local, regional, and national jurisdiction. They are required to establish, maintain, and report compliance to regulators on one hand, and to enforce policies and procedures internally to fulfill business requirements on the other hand, satisfying internal users in terms of security, availability, and performance regarding IT functions at the same time [71]. Regulatory standards and acts serve as the bases for examining risks associated with IT usage, for instance, Sarbanes-Oxley Act (SOX), Graham-Leach-Bliley Act (GLBA), EU Data Protection Directive (EUDPD), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI), and Basel II. However, due to the complicated mapping between SOX, COSO, and COBIT regarding the IT control objectives, little literature discusses the ever increasingly important role of IT controls to ensure compliance.

SOX was enacted with the aim to strengthen internal controls over financial reporting of U.S. public companies. SOX Section 404 mandates corporate executives to attest the internal control effectiveness, to report to the public the material weakness in internal controls, and to have the report assured by certified public accountants (CPA). Although SOX does not address IT directly, its implication for IT is significant, covering almost all transactions and financial data flowing through IS within an organization. It makes management responsible for the integrity of financial information by assessing IS and processes. The application of the COBIT framework in SOX compliance has made the integration among compliance, internal controls, and risk assessment realized. The regulation regarding internal controls issued by SEC and PCAOB are the direct result from SOX. SEC final rule requires management to consider IT-related risks and controls based on internal control framework such as COSO [21]. PCAOB Standards No. 2 reinforces the crucial role of IT in internal controls — how company use IT and how it has influenced internal controls over financial reporting [39]. The influential power of SOX has driven IT controls to a crucial position in helping organizations to fulfill the stringent requirements of regulations [31].

Internal Control Implementation in China

The advancement of informatization in China has reached the same level as western countries. The Chinese Specific Independent Auditing Standard No.28 describes ITGC as the IT policy, and the SOX procedures about networks, operational systems, databases, applications, and related personnel as effective controls to ensure the smooth operation of IS [56]. However, research on internal controls in China is comparatively lagging, which has caused insufficient attention being paid to the relationship between IT and internal controls [13, 53, 83, 84]. Many enterprises in China are facing issues in the IT control area, such as IT plans and business process and objectives not aligned, and the misinterpretation of control policies and frameworks. IT and business processes should be integrated and the evaluation of IT control effectiveness must be emphasized [34]. Huang et al. [35] proposed an ITGC evaluation model under COSO-ERM framework to assess the soundness of IT control environment. The effectiveness of ITGC should be assessed with regard to market standards, e.g., US government enacted SOX to measure the effectiveness of IT control. Without third party monitoring, IT control effectiveness cannot be assured [86].

Five central government departments in China including the Ministry of Finance, China Securities Regulatory Commission, National Audit Office, China Banking Regulatory Commission, and China Insurance Regulatory Commission co-issued the Basic Norms in June 2008, which is known as “The China SOX Act”. Subsequently, the Guidelines were introduced in April 2010. The Basic Norms were applied to Chinese listed companies since 2012. The implementation of the Guidelines means that information of internal controls of

listed companies in China has to be disclosed to investors. The Basic Norms provides an internal control framework comprising of the control environment, risk evaluation, internal control activities, information and communication, and control monitoring. Listed companies are required to evaluate the effectiveness of internal controls and to issue self-assessment reports on the effectiveness of the firm's internal control systems. An audit report on internal control effectiveness is to be provided by the certified public accountant (CPA). No. 18 of the Guidelines specifically talks about IT controls over enterprise's IS.

CONCEPTUAL MODEL AND HYPOTHESES

Research Constructs

Appendix A provides the definitions of the three constructs and their respective dimensions and indicators:

- ITGC: This research adopts the IT Control Objectives of Sarbanes-Oxley [40], a research by ITGI intended for management and assurance professionals to evaluate an organization's IT controls, as an important reference. ITGC comprises of five controls over IT control environment, computer operations, access to programs and data, program development, and program change. Similar processes of ITGC was adopted by Chan and Lao [11] in the evaluation of the business value of ITGC.
- Compliance: Regulatory compliance describes the goal that organizations desire to achieve with an effort to warrant their awareness and actions to comply with relevant laws and regulations. In the U.S, how companies perceive compliance is significantly influenced by SOX legislation [3, 69]. This research adopts the six different components of IT compliance ─ data retention, data protection, corporate governance, intellectual property, legal framework, and national security proposed by Symantec [73].
- IT-related Risk: According to The Risk IT Framework, IT-related risks are the business risks relating to the use, operation, ownership, influence, and involvement of IT [38]. This research adopts the four dimensions of IT-related risks based on Symantec's IT Risk Management Report which includes security risk, availability risk, performance risk, and compliance risk [54, 73].

Research Model

Figure 1 shows the research conceptual model. Despite the perceived links between ITGC, regulatory compliance, and mitigation of IT-related risks, practical guidance and empirical evidence are lacking in this area. Few attempts have ever been made to empirically test the proposed concept, particularly on the effect of ITGC and its effectiveness. Effective ITGC directs organizations to comply with increasing regulatory requirements, with the mitigation of IT-related risks as a critical objective [78]. Though compliance is a must, many organizations have encountered disastrous failures when focused on only compliance rather than on both compliance and IT risk management [6]. Such incidents imply that compliance cannot assure risk-free environment and ITGC may not support the mitigation of IT-related risks.

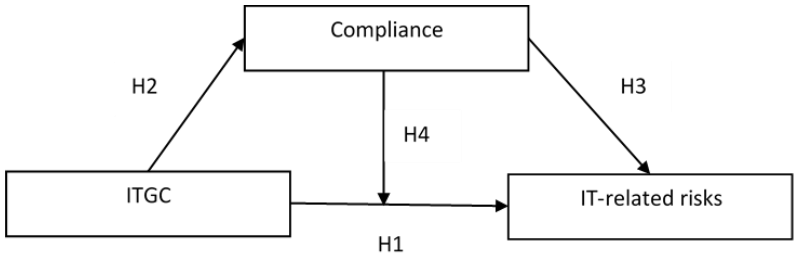


Figure 1: Research Conceptual Model

This research model draws upon the widely acknowledged frameworks for synthesizing and guiding ITGC and risk management. Dehning and Richardson [17] developed a research framework that studies the contribution of IT to business value. The framework indicates that various IT constructs affect firm performance through direct and indirect ways. Specifically, the indirect way is realized when IT investment is transformed to intermediate business process improvements and then leading to overall performance. Such framework enables the drawing of inferences about the direct and indirect effects of ITGC ─ the implementation of ITGC can facilitate compliance effort, which then leads to better mitigation of IT-related risks. In other words, IT compliance objective can be achieved through effective implementation of ITGC, which further reinforce management of IT-related risks.

Hypotheses Development

First, an examination of the direct impact of ITGC on IT-related risk mitigation is carried out. Pirta and Strazdina [63] noted a negative relationship between IT control environment and IT-related risks. The 2013 Federal CFO Insights states that the main criterion when designing internal controls is the consideration of risks [18]. From the perspective of decision makers, internal controls is a system to assess, reduce, and limit risks related to business processes, information technology applications, and information dissemination [69]. IS security and controls protect data, information, and applications from illegal access and damage, and secure their integrity and availability [76]. On the other hand, weak IS security would not prevent threats from unauthorized users accessing the systems and modifying data [64]. Klamm and Watson [44] uncovered that firms having material weaknesses in IT controls would encounter a broader span of issues over multiple internal control elements. Strong IT capability signals lower IT-related business risks [12]. These discussions lead to H1:

H1: ITGC has a direct mitigating effect on IT-related risks.

Next, an examination of the contribution of ITGC to IT compliance management follows. Meyer [55] asserted that when performing business process entry, compliance is assured with embedded controls. SOX compliance has driven organization to build strong IT governance model in order to meet business requirements on accountability and responsiveness. As a result, more efficient and effective operations under ITGC implementation bring about benefits such as complying with regulatory requirements, enhancing operations through integrating security, availability, performance, and optimizing risk management scheme [31]. COSO framework conceptualized the link between IT control and compliance, indicating that internal controls help ensure compliance with applicable business regulations in the market [14]. Bone [8] expressed that SOX compliance could not be assured without considering IT systems, a core element of the internal control environment. Thus, it is postulated that ITGC support regulatory compliance.

H2: ITGC is positively related to the compliance with laws and regulations.

Then, an examination of the effect of regulatory compliance over IT-related risk mitigation is carried out. Literature review shows that compliance with SOX requires risk assessment and development of internal controls, including controls over IS. Regular ITGC evaluation and audit in response to regulatory compliance requirements can help reduce risks and prevent organizations from suffering financial and reputation damages. Hardy [31] concluded that SOX and other global regulations foster a strong IT governance model, leading to efficient and effective operations which also include optimized risk management. The role of compliance is strategic in terms of providing governance to organizations toward a wide dimension of risks and developing an enterprise-wide risk management function [60]. It is expected that regulatory compliance has a mitigating effect of IT-related risks. This leads to H3:

H3: Regulatory compliance is negatively related to an organization's exposure to IT-related risks.

Finally, the mediation effect of compliance between ITGC and IT-risk mitigation is assessed. The framework developed by Dehning and Richardson [17] enables inferences to be drawn ─ IT compliance objective can be achieved through effective implementation of ITGC, which further reinforce the management of IT-related risks. This leads to H4:

H4: IT compliance has a mediating effect over the relationship between ITGC and IT-related risks.

RESEARCH METHODOLOGY

Research Instrument Development and Validation

In order to ensure content validity, a review of previous literature was conducted [25]. A field study in China was followed to empirically validate the research

model. A research instrument was synthesized for data collection. It consists of three main parts to reflect measurement constructs of the model (ITGC, compliance, and IT-related risks). The original version was developed in English with measurements adopted from published reports and literature. Moreover, to facilitate respondents' comprehension, a Chinese version was also developed. Back-translation technique was employed to ensure the linguistic equivalence [57].

To assess the logical consistency, relevance, and items sequencing, a small-scale pre-test of the instrument was performed [25] with consultants working at internal controls, risk management, and IT risk assurance functions. Interviews with professional consultants were conducted to assess the content of the measuring items for ITGC, compliance, and risk management. Professionals were asked to comment on the relevance of research constructs and to assess the sufficiency of the measurement items of the constructs. Based on comments identified by respondents, the questionnaire was adjusted accordingly. Through this refining exercise, it is believed that measurement errors could be reduced and the validity of the measurement items could be improved.

Data Collection

To proceed to data collection, respondents were invited from both IT and business areas to avoid potential bias in single-sided data. A questionnaire survey has been adopted to collect data for analysis. Respondents had to rate each question on a 7-point Likert scales, which a higher score signifying stronger agreement with an assessment item ─ (1) strongly disagree, (2) disagree, (3) somewhat disagree, (4) neither agree nor disagree, (5) somewhat agree, (6) agree, and (7) strongly agree. The survey was conducted in China with companies including Chinese private enterprises, Chinese state-owned enterprises (SOE), foreign-owned enterprises, and joint ventures. Target companies are not restricted to listed companies. Target respondents are senior management from both IT and business departments who are holding positions such as IT senior manager, compliance manager, IT internal audit senior managers, general manager, finance controller, operation senior manager, etc. as they should have the knowledge and experience of their companies in the research area. Respondents from a variety of industries such as manufacturing, financial services, insurance, real estate, banking, communications, retail and consumer goods, and others were invited to ensure the generalization of market opinion. Data collection was conducted via email and on-line survey platform. 112 respondents were contacted for the survey. After eliminating invalid responses with straight lining and outlier cases, a total of 100 valid responses were collected, resulting in a valid response rate of 89%. Respondents have an average of 6-10 years of working experience in their respective domain. This suggests that respondents have sufficient competence to answer questions on the subject matter.

Analysis of Respondents

The collected demographic information of respondents and their respective organization characteristic are shown in Table 1. It is noted that:

- Company ownership: The largest portion (39%) of respondents is from state-owned enterprises, followed by private enterprises (30%), and wholly foreign owned enterprises ("WFOE") (20%).
- Industry: Respondents are from various industries including financial services (21%), telecommunications (15%), information technology and services (14%), wholesale or retail-consumer goods (10%), and others (35%).
- Company size: 62% of respondents are from large company with employees over 1000. Respondents from medium (200-999 employees) and small (below 200 employees) size companies are equally allocated.
- Years of working experience: 50% of respondents gained more than 9 years working experience in their fields, among which 15% have over 12 years. Respondents with 6-8 years working experience accounts for 21%, whereas respondents with the least working experience (3-5 years) accounts for 29%.
- Department: 36% of respondents are working in the IT departments, finance personnel accounts for 24%, followed by risk management (10%), general management (10%), and internal audit (8%).
- Position: Respondents who hold positions in senior management level are 35%, with 12% being the company director or executive. Middle management accounts for 39%. 26% are the system engineers or IT administrators.

Analytical Methods

Data validation was carried out with partial least squares (PLS) drawing on SmartPLS2.0. With the

following reasons, it is rational to apply PLS in this research:

- PLS is a variance-based SEM technique which widely applied in previous IS studies;
- As all constructs draw on a formative measurement model set-up in the research, PLS suits this study well;
- The model include hierarchical component with formative "first-order" or "lower-order" and an aggregate "second-order" or "higher-order" constructs. PLS is suitable for the estimation of this kind of model;
- The use of PLS suits when there is scarce theoretical knowledge about a topic. Insofar, there have been very few empirical studies in the research context and limited prior literature. This study investigates research questions with limited prior theory thus using PLS is appropriate.

Table 1: Sample Characteristics and Key Information of Respondents

Organization Characteristic	**Frequency**	**Respondent Key Information**	**Frequency**
Ownership structure	39	**Years of Experience**	
State-owned	20	3-5	29
WOFE	3	6-8	21
Joint venture	30	9-11	35
Private	8	12-15	10
Other		>15	5
Industry		**Function**	
Financial services (Bank, Insurance and Securities)	21	Information Technology	36
Real estate	5	Internal Audit	8
Telecommunication	15	Risk Management	10
Wholesale/Retail-consumer goods/Trading	10	Finance	24
Information Technology and Services	14	General Management	10
Chemicals	3	Others	12
Food Production	4	**Position**	
Electronic Manufacturing	5	System Engineer/IT Administrator	26
Leisure, Travel and Tourism	4	Department/Project Supervisor	18
Oil and Energy	6	Manager	21
Others	13	Senior Manager	23
Firm size		Senior management/ Director, Executive	12
<50	5		
50-99	7		
100-199	7		
200-299	4		
300-499	4		
500-999	11		
1000-2000	7		
>2000	55		

The exogenous latent variable is ITGC and the two endogenous variables are compliance and IT-related risk. Compliance mediates the relationship between the exogenous construct, ITGC, and the endogenous construct, IT-related risks. Formative measurement represents instances where the indicators cause the construct. The constructs in this research are set as formative based on the following rules [42]:

- Causality is observed from indicators to constructs.
- Indicators are not interchangeable.
- No covariation among indicators is observed.
- Indicators differs nomologically.

The measurements for ITGC and IT-related risk are multidimensional. Under the repeated indicators approach, higher-order latent variables link to all manifest variables of lower-order constructs. This approach repeats the number of manifest variables used in order to represent the higher-order constructs (HOCs) [70]. The formative conceptualization of ITGC as a HOC is based on the logic that improvement in IT control environment, computer operations, access to programs and data, program development, and program changes enhance ITGC. Similarly, IT-related risks are assessed by four different dimensions, i.e., security, compliance, availability, and performance, which are sufficient to represent an organization's overall exposure to IT-related risks. Six formative indicators to assess compliance includes data retention, data protection, corporate governance, intellectual property, legal framework, and national security. The PLS-SEM guidelines were followed to assess the measurement models before evaluating the structural model [28]. Convergent validity, multi-collinearity, weights and their level of significance for the formative construct, compliance, and for the HOCs, ITGC and IT-related risks, were checked [43].

ANALYSES AND DISCUSSIONS

Measurement Model Evaluation

Convergent validity

Convergent validity measures the correspondence between similar constructs. Separate redundancy analysis for each LOC and HOC to assess the convergent validity of formative constructs were carried out. The questionnaire contains global single-item measures with generic assessment of all formative constructs. A single item as an alternative measurement was applied. A correlation of 0.8 or higher is expected [62]. The redundancy analysis result is shown in Table 2. Except for ITCE, PC and PD, the path coefficient for all the rest are above the threshold of 0.8. As ITCE (0.792), PC (0.795), and PD (0.797) are marginal, the formatively measured constructs are still considered to have sufficient degree of convergent validity. As a result for the first-order measurement model, the analysis demonstrates that the measures are reliable with adequate convergent validity.

Table 2: Redundancy Analysis Result

HOCs	Path Coefficient	LOCs	Path Coefficient
ITGC	0.826	ITCE	0.792
		APD	0.913
		PC	0.795
		PD	0.797
		CO	0.814
COMP	0.841	COMP	0.841
ITRR	0.837	AR	0.818
		CR	0.885
		PR	0.821
		SR	0.849

Table 3: Variance Inflation Factor Results

ITGC				Compliance		ITRR			
Indicators	**VIF**	**Indicators**	**VIF**	**Indicators**	**VIF**	**Indicators**	**VIF**	**Indicators**	**VIF**
ITCE	3.349	ITCE_1	3.162	COMP_1	2.436	AR	3.258	AR_1	1.831
		ITCE_2	3.643	COMP_2	3.671			AR_2	1.831
		ITCE_3	2.134	COMP_3	3.187	CR	2.370	CR_1	2.165
		ITCE_4	2.557	COMP_4	2.430			CR_2	2.165
		ITCE_5	2.121	COMP_5	2.206	PR	2.708	PR_1	2.686
APD	1.833	APD_2	2.562	COMP_6	1.893			PR_2	2.686
		APD_1	2.562			SR	3.199	SR_1	2.423
PC	4.634	PC_1	3.006					SR_2	2.423
		PC_2	3.662						
		PC_3	2.559						
PD	3.751	PD_1	3.682						
		PD_2	3.682						
CO	3.814	CO_1	2.113						
		CO_2	2.113						

Collinearity

The level of collinearity was assessed by computing the variance inflation factor (VIF) for the five dimensions of ITGC (IT control environment, access to program and data, program development, program change, and computer operations), the four dimensions of IT-related risks (security, availability, performance, and compliance), and the six indicators of compliance (data retention, data protection, corporate governance, intellectual property, legal framework, and national security). Appendix A presents the constructs and measurement items. Table 3 shows the VIF values (using IBM SPSS Statistics). All VIF are lower than the threshold value of 5, suggesting that the collinearity of all formative constructs are not up to the critical level and there is no issue with the estimation of PLS path model [62].

Significance and relevance of formative indicators

To test the outer weights (relative importance) and outer loadings (absolute importance) of indicators [25], the bootstrapping procedure drawing 5000 subsamples from 100 cases was adopted. Construct validity was assessed with the significance of weightings and corresponding outer loading (threshold is 0.5) [10]. Indicator weights of ITCE, APD, PC, PD, CO, AR, SR, CR, PR, and COMP range from 0.025 to 0.836. Dimension weights for ITGC and ITRR range from 0.188 to 0.292. The bootstrapping results provide evidence that the formative indicators weights for ITCE_2, ITEC_3, ITCE_4, COMP_3, COMP_4, CR_2 are not high and not significant ($p \leq 0.05$). However, the corresponding item outer loadings are relatively high (i.e., >0.50). Outer loadings of a formative indicator are considered as the absolute contribution toward the construct. With prior research providing support to the relevance of these indicators for capturing the dimensions of ITGC, COMP and ITRR, these items are interpreted as absolutely important and indicators were retained [28]. Table 4 presents the outer loadings and corresponding *t*-values. Weights of formative indicators and dimensions are presented in Appendix B. Overall, the above analysis suggests sound properties for the formative constructs at both 1st order and 2nd order level.

Table 4: Outer loadings of indicators with nonsignificant outer weights

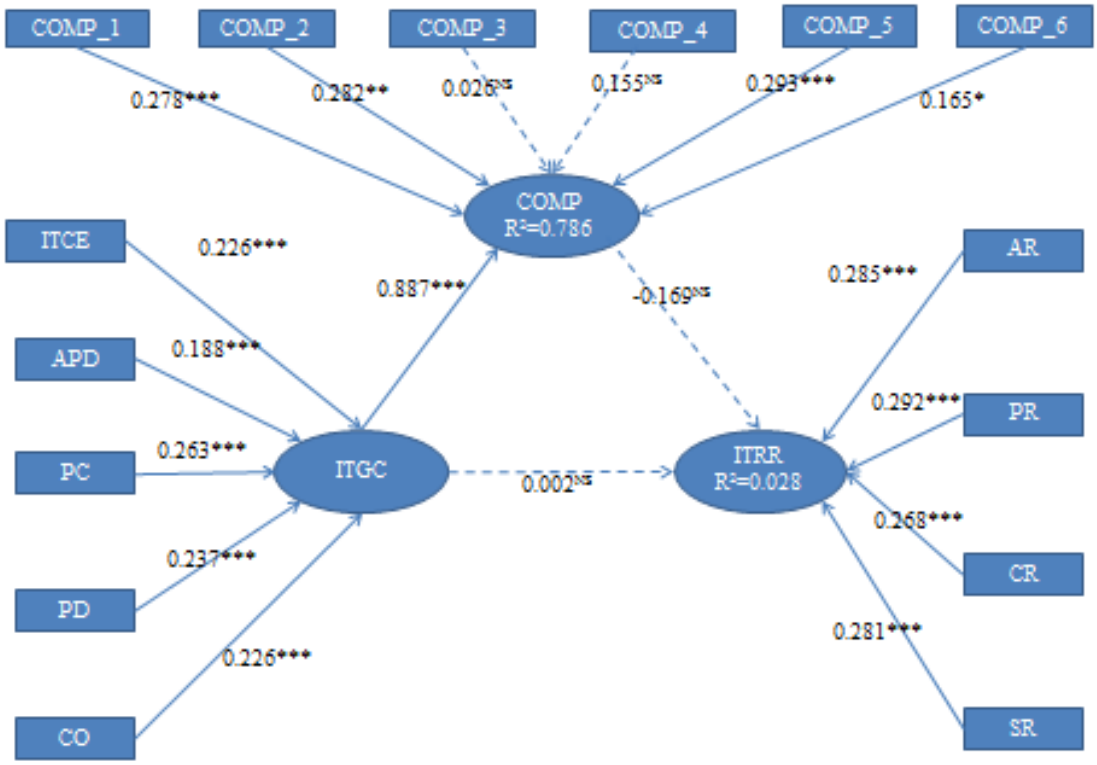
	Loadings	***t*-value**
COMP_3 -> COMP	0.906	28.774
COMP_4 -> COMP	0.835	16.057
CR_2 -> CR	0.807	11.308
ITCE_2 -> ITCE	0.823	9.0392
ITCE_3 -> ITCE	0.922	23.37
ITCE_4 -> ITCE	0.915	31.999

Structural Model Evaluation

After proving the validity and reliability of the construct measures, the structural model evaluation

follows. Path coefficients are estimated by ordinary least squares regressions. Results may be biased if collinearity is present [28]. The same method as in the assessment of measurement model (adoption of VIF) to examine the structural model for collinearity issues between ITGC and compliance was first applied as they serve as exogenous constructs in the prediction of IT-related risk. VIF of both were 4.911, slightly below the threshold of 0.5. Therefore the structural model results are not negatively affected by collinearity.

The hypotheses were tested by examining the significance of paths in the model and the R^2 values [4]. The priori statistical power of the two dependent variables (compliance and IT-related risks) were calculated. Bootstrapping was used to assess the significance and relevance of the structural model. Upon examining the predictive power of compliance, a substantial R^2 value of 0.786 resulted while the prediction of ITRR is weak (R^2=0.028). Results from the bootstrapping procedure (100 cases, 5000 samples, no sign changes option) reveal that one of the three structural relationships is significant (p≤0.05). The result in Figure 2 highlights the important role of ITGC to compliance with path coefficient 0.887. However, compliance has weak negative effect on IT-related risk with a coefficient of -0.169. ITGC has almost no effect on IT-related risk (0.002). The above results support H2, while H1 and H3 are rejected (Figure 2). As H1 and H3 are not supported, the mediation effect of compliance (H4) is rejected as a consequence.



Notes: NS=not significant. ***p≤0.01; **p≤0.05; *p≤0.10; dashed lines represent non-significant relationships. COMP=Compliance; ITRR= IT-related risk

Figure 2: PLS-SEM estimates

Post-hoc Analyses

A post-hoc analysis was conducted to investigate the effect of compliance on ITGC. The analysis result supports the argument that compliance affects ITGC implementation. The examination shows a substantial R^2 0.784. It implies that 78% of the variance in ITGC is explained. Table 5 demonstrates that compliance is significantly related to ITGC with path coefficient of 0.886.

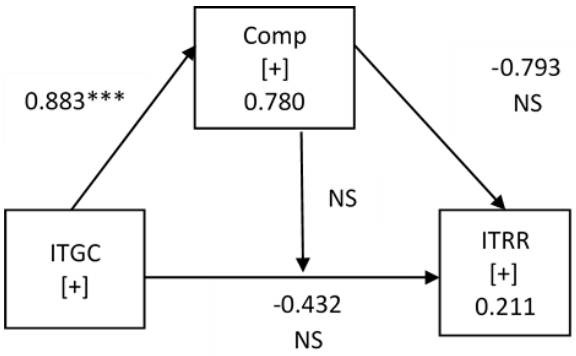
Table 5: Significance testing results of the effect of compliance on ITGC

	Path coefficient	***t*-values**	**Significance levels**	***p*-values**
COMP→ITGC	0.886	21.864	***	0.000

Notes: NS=not significant. ***$p\leq0.01$; **$p\leq0.05$;*$p\leq0.10$

Partial least squares multigroup analysis was performed (PLS-MGA) [32] to investigate whether there is a difference between enterprises of various ownership structures exist in the model. Three groups of enterprise structures, namely state-owned enterprises (SOE), foreign enterprises (wholly foreign-owned enterprises (WFOE) and joint ventures (JV)), and private enterprises were included in the analysis because they are the three dominant groups in the sample data set. Building on PLS-SEM bootstrapping results, the method provides non-parametric significance test for the difference in path coefficient. The following figures show the results for ownership-specific path.

H2 is supported for state-owned enterprises. H1, H3, and H4 are rejected. See Figure 3.

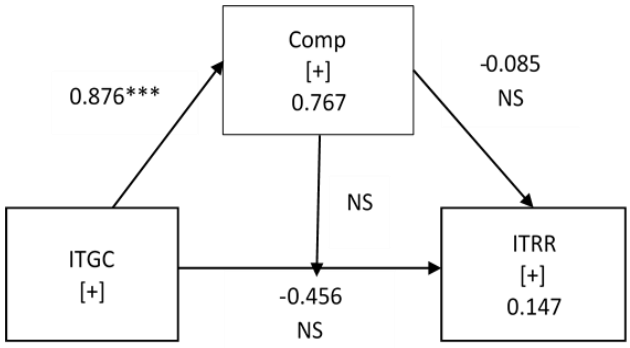


Notes: NS=not significant. ***$p\leq0.01$;**$p\leq0.05$; *$p\leq0.10$

Figure 3: State-owned enterprises PLS-SEM estimates

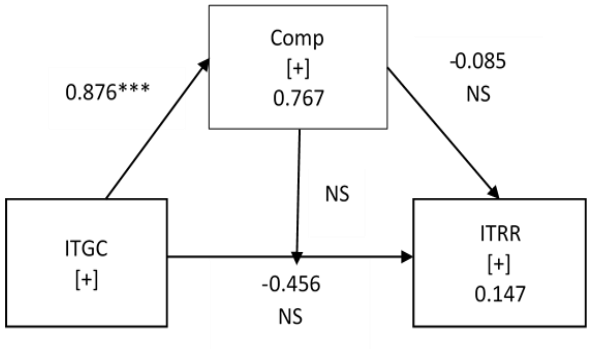
H2 is supported for foreign enterprises. H1, H3, and H4 are rejected. See Figure 4.

H2 is supported for private enterprises. H1, H3, and H4 are rejected. See Figure 5.



Notes: NS=not significant. ***$p\leq0.01$; **$p\leq0.05$;*$p\leq0.10$

Figure 4: Foreign enterprises PLS-SEM estimates



Notes: NS=not significant. ***$p\leq0.01$; **$p\leq0.05$;*$p\leq0.10$

Figure 5: Private enterprises PLS-SEM estimates

Findings

The analyses above show that ITGC and regulatory compliance are positively related and interacting with one another. ITGC help Chinese enterprises comply with laws and regulations. At the same time, the latter drive further development of ITGC in Chinese enterprises. The quality and effectiveness of ITGC signify stronger control environment and successful compliance [75]. Financial scandals have brought about rigorous rules governing IS audit and control which organizations must follow [66]. Thus, ITGC and compliance are positively associated and that they are critical elements of nowadays business environment. However, analysis results also reveal that ITGC implementation in organizations shows little contribution

to the mitigation of IT-related risks. Compliance success does not significantly related to organizations' exposure to IT-related risks either. It is further concluded that compliance does not have a mediating effect on the relationship between ITGC and IT-related risks. When considering ownership structure, all structures show significant relationship between ITGC and compliance. However, both compliance and ITGC of all ownership structures do not show effective mitigation of IT-related risks.

Companies in the survey generally consider ITGC help meeting relevant compliance requirements. Yet enterprises with ITGC satisfying regulatory compliance do not recognize well-managed IT-related risks profile. In theory, the implementation of effective internal control systems is helpful in reducing corporate risks. But when compliance is the pure objective, the design and operation of ITGC may not serve the intended functional purpose. This study uncovers facts about the unique situation of ITGC implementation in China, which explains the deviation from hypotheses. Answers to the two proposed research questions are presented as follow:

1. *Does ITGC implementation in Chinese enterprises contribute to the mitigation of IT-related risk?*

Analysis results show that ITGC implementation in Chinese enterprises does not contribute to the mitigation of IT-related risk. The Chinese regulatory authorities introduced "China SOX" requiring listed companies to respond to the internal control soundness by disclosing self-assessment report annually and with appointed CPA to issue assurance report on internal controls. Effective and regular evaluation of internal controls is an important and necessary activity for effective implementation. However, neither internal control information nor IT-related issues of internal controls were properly disclosed as expected. Many Chinese enterprises did not recognize or were not able to detect the internal control deficiency of their established internal control systems.

For instance, 13.8% US listed companies disclosed internal control deficiency in their internal control self-assessment reports in 2014 [52]. In China, however, only one IT control deficiency was disclosed among listed companies between 2012 and 2014 [47]. The small number of defects in IS does not mean that the reliability of IS security and control operations in Chinese enterprises was high. This is probably because studies and practices in the area of IT controls and audit are still relatively lagging in China [36]. As such, ITGC only reveals the tendency for compliance but plays no actual role as to mitigate business risks and IT-related risks. Listed companies in Shenzhen main board disclosed almost no internal control material weaknesses between 2009 to 2011, while that in the U.S. was 16.9% [51]. According to the Internal Control White Paper 2011 of Chinese listed companies, less than 1% companies disclosed internal control deficiencies in their voluntary internal control self-assessment reports. Among the 99% of companies that claimed having effective internal control systems in their self-assessment report, many of them actually had serious control deficiencies and their internal control systems were substantially ineffective. 50 listed companies were penalized for violation against laws, accounting for 2.38% of the total listed companies in that year.

It is apparent that Chinese enterprises implementing internal controls and disclosing internal control information only to comply with enforced rules and regulations. Little or no objective of risk mitigation has been identified in their internal control plans [49]. Also, the disclosure of internal control information is largely a formality with no substantive content [50]. Hao and Rainsbury [30] pointed out that Chinese listed companies which had complied with legal requirements showed effective internal controls but the substance and quality was poor especially in terms of internal control deficiencies and remedial actions. This can be attributed to the fact that the development of enterprise internal controls as well as concerned rules and regulations have relatively short history in China, lacking business-related practices [77]. Consequences of such also led to 97% of internal control audit reports of listed companies in China 2013 were issued with unqualified opinion, lacking clear evaluation criteria and substantive content [52]. This percentage is much higher than that in the U.S. where companies have comparatively stronger internal control systems. With a high number of CPA assurance reports with unqualified comments in China, it is clear that the ability to identify material weakness and the willingness to disclose material defects in Chinese enterprises are to be enhanced [47]. And as a result, it is neither expected that ITGC, one of the core elements of internal controls, is held in high regard.

2. *What role does compliance play in the relationship between ITGC and mitigation of IT-related risk?*

The original purpose of regulatory compliance toward enterprise IS is to reduce IT-related risks. But compliance does not show to have significant negative relationship to IT-related risks in the analysis results. Legal compliance is a state requirement to improve the soundness of businesses and their responsibility to the market. The mitigation of risk of any kind is considered

as business/operation objectives. Even though this research instrument is designed based on the COSO-ERM framework which applies risk-based approach, with no risk mitigation as the foundation of ITGC implementation in China, compliance and risk mitigation can only be considered as two independent issues with no significant relationship or connection. It may also be interpreted that ITGC implementation in Chinese enterprises is not effective enough. At present, compliance with laws and regulations in China cannot help to reduce corporate IT-related risks. It is not surprising to see Chinese enterprises of full compliance encounter serious business failure because they focus on compliance rather than risk management and, in particular, IT risk management. [50]. Chinese enterprises are in the stage of gradual transition from responding to regulatory authorities to corporate risk management and the process takes time and effort [85].

CONCLUSIONS

This study uncovers the fact that Chinese enterprises have been over-focusing on complying with regulatory requirements while the goal of ITGC, i.e., IT-related risk-mitigation, has been neglected. "Effective" ITGC helps enterprises meet regulatory requirements which, in turn, should promote a stronger IT control environment. However, developing "effective" ITGC for Chinese enterprises requires joint efforts from enterprises, research as well as regulatory institutes. Information and knowledge sharing among these sources may reduce the learning cycle and costs, and help to build and set required standards in the market.

Fully compliant Chinese enterprises which encountered headline-grabbing failures implies that the objective of regulatory compliance should not be regarded as ultimate goal of IT controls. Risk management should be carried out simultaneously. This research also reveals the fact that Chinese enterprises are not willing or not able to manage risks. To avoid high associated disclosure costs, companies attempted to cover up deficiencies [1]. Such attempt did not really achieve its objective but accumulated more problems and consequently led to business failure [50]. IT controls and the control environment should be established by taking into account the broader context of risk management. According to CCW Research, a leader of IT market research and consultancy in China, 85% Chinese companies still need to strengthen IT management and control ability [82]. IT controls in Chinese enterprises are not operating effectively, which easily trapped enterprises into risks. Incompetent IT management and IT control capability have become bottlenecks for sustainable development, particularly in small and medium-sized enterprises in China. Face interviews again with respondents of the survey instrument pretest have concluded the following:

- Top management are not giving sufficient attention to IT controls in Chinese enterprises. Many of them neither have the knowledge of ITGC as an element of internal controls nor have the knowledge of IT and business alignment. They have not fully realized the crucial role of developing IT controls for business sustainable development in a high-risk era [81]. As a result, ITGC cannot help companies achieve the goal of reducing IT-related risks but rather become a heavy and costly burden.
- Companies operating in China lack advanced IT control practical guidance and talents. IT-related control frameworks such as COBIT and ISO20000 were introduced into China relatively late. Compounded with the problem of inadequate research and development of IT controls in China, few companies can effectively apply ITGC in their business environment properly.
- Many Chinese enterprises are devoting full energy in the development of core business systems, such as enterprise resource planning systems, customer relationship management systems, and supply chain management systems, while IT controls are not considered as urgent needs. With what these enterprises have learnt from new IT controls standards and regulatory requirements, schedules for incorporating ITGC into their IS projects were drawn, but not an immediate concern.

Implications

This study empirically developed its measures in a nomological network. The research is exploratory in nature which presents a deeper understanding of ITGC implementation status in China. Though the results are limited to Chinese enterprises, this study presents novel findings to MIS and business management research in particular to the association between IT-related risks and IT control capability and quality.

This study has also brought about a number of interesting managerial implications:

- Though ITGC are developed and implemented by the IT department, it does not mean that business managers should keep themselves away from such. Business and IT alignment should be expected. It

should be understood that IS support business operations or even play a strategic role. Deficiencies in or problems with IS may result in, not only IT-related risks but, business risks. Business managers and IT managers should work together to design and implement desired ITGC to support the business.

- As it is uncovered that Chinese enterprises have weak awareness in risk mitigation, it is suggested that both business and IT managers should learn more about risk management. Business management should consider ITGC from a risk-based view by asking questions like what are the known risks, what steps have proven effective in mitigating the known risks, how should conformance to those mitigating activities be measured, and what should be reported to the public? To take a step further, businesses should achieve IT governance with goals to ensure good value from investments in IT and mitigating IT-related risks [67].
- Organizations are suggested to establish robust compliance and internal audit functions so as to practice risk management and create an effective control environment. The compliance function should identify and assess risks, design and implement internal controls, monitor and report on the effectiveness of controls, resolve compliance difficulties as occurred, and advise the business on rules and controls [37]. With IT governance as the objective, business and IT management can be logically integrated.
- Other than managerial staff who should have appropriate concepts and knowledge of risk management and IT controls, operational staff should realize the purpose and importance of such. An effective risk culture plays a critical role in determining the health and performance of an organization. While organizations are struggling in short-term economic pressure, it is necessary to focus on improving risk management within the existing organization culture by understanding the culture and then designing a culturally sensitive enterprise risk management program. Different organization may have to tailor-make their own program according to their context and resources. The desired risk management program should be comprehensible, transparent, and with visible role-modelling of desired behaviors and standards by senior management [5]
- Besides the China SOX, globally recognized IT governance frameworks and standards, such as the COBIT, ITIL, and ISO/IEC 27000-series, may provide Chinese enterprises with guidance for IT-control environment and IT governance.

Limitations and Future Research

ITGC dimensions adopted in this research may not be suitable for some companies and industries in China as different markets may have unique requirements. As suggested by ITGI, organizations should carefully consider necessary IT control objectives based on their specific circumstances. Thus, further research in this topic can be implemented with tailor-made ITGC dimensions for different Chinese markets. Next, restricted by the limited information of this topic in China, objective arguments and generalized comments may bring about more rigorous research input and result. Interviews and case studies may also be considered to improve the quality of the research. Lastly, it is possible that other factors may also influence the effect of ITGC effectiveness and compliance on IT-related risks. Future research may work into such direction to identify further information for market participants in China.

REFERENCES

[1] Arnold, V., Benford, T., Canada, J. and Sutton, S. G. "The role of enterprise risk management and organizational strategic flexibility in easing new regulatory compliance," *American Accounting Association Annual Meeting*. 2009.

[2] Bae, B. and Ashcroft, P. "Implementation of ERP systems: accounting and auditing implications," *Information System Control Journal,* Volume 5, Number 4, 2004, pp.43-48.

[3] Baker, R., Bealing Jr., W. E., Nelson, D. A. and Blair Staley, A. "An institutional perspective of Sarbanes-Oxley Act," *Managerial Auditing Journal*, Volume 21, Number 1, 2006, pp. 23-33.

[4] Barclay, D., Higgins, C. and Thomson, R. "The partial least squares approach to causal modeling, personal computer adoption and use as an illustration," *Technology Studies*, Volume 2, Number 2, 1995, pp 285-309.

[5] Barkley-Levensona, E.E., Leijenhorsta, L.V. and Galván. A. "Behavioral and neural correlates of

loss aversion and risk avoidance in adolescents and adults," *Developmental Cognitive Neuroscience*, Volume 3, January 2013, pp 72–83.

[6] Barnier, B. "Managing IT business risk," *The Journal of Corporate Accounting and Finance*, Volume 22, Issue 6, 2011 (September/October), pp. 65-68.

[7] Bellino, C., Wells, J., Hunt, S. and Horwath, G. "GTAG 8: Auditing Application Controls," *The Institute of Internal Auditors*, 2007.

[8] Bone, J. "Managing IT controls for Sox compliance," https://www.complianceweek.com/blogs/james-bone/managing-it-controls-for-sox-compliance#.WzS2edUzbX4, Nov 2016.

[9] Carcary, M. "Developing a framework for maturing IT risk management capabilities", *Proceedings of 6th European Conference on Information Management and Evaluation*, Cork, 13-14 September 2012.

[10] Cenfetelli, R. T., and Bassellier, G. "Interpretation of formative measurement in information systems research," *MIS Quarterly*, Volume 33, Number 4, 2009, pp. 689-708.

[11] Chan, W. H. B., and Lao, S., K. "A study of the business value of ITGC in China", *Journal of Information Technology Management*, Volume XX Number 4, 2009, pp. 22-36.

[12] Chen, Y., Smith, A. L., Cao, J. and Xia, W. "Information technology capability, internal control effectiveness, and audit fees and delays," *Journal of Information System*, Volume 28, Number 2, 2014, pp 149-180.

[13] Chen, Z. "Approach to corporate internal control framework in the informationized ecological environment," *Accounting Research*, 2007-01.

[14] COSO. "Committee of Sponsoring Organizations. 2004a", *Enterprise risk management-integrated framework: executive summary framework*, NJ: AICPA.

[15] COSO. "Committee of Sponsoring Organizations. 2004c," *Applying COSO's enterprise risk management-integrated frame work*, September 29 slideshow.

[16] COSO. "Committee of Sponsoring Organizations of the Treadway Commission (COSO)", *Internal Control—Integrated Framework*, 2011.

[17] Dehning, B. and Richardson, V. J. "Returns on investments in information technology: A research synthesis," *Journal of Information System*, Volume 16, Number 11, 2002, pp. 7-30.

[18] Deloittee. "Federal CFO Insights: aligning internal control and enterprise risk management framework", 2013.

[19] Edelstein, S. M. "Sarbanes–Oxley compliance for non-accelerated filers," *CPA Journal*, Volume 74, Number 12, 2004, pp. 52-59.

[20] Elky, S. *An Introduction to information system risk management*, SANS Institute, 2006.

[21] Fitzsimons, A. P. and Thompson, J. W. "Final rules on management's reports on internal control and on Influencing the conduct of audits," *Bank Accounting and Finance*, Volume 16, Number 6, 2003, pp. 43-49.

[22] Flowerday, S. and Von Solms, R. "Real-time information integrity - system integrity + data integrity + continuous assurances," *Computers and Security*, Volume 24, Number 8, 2005, pp. 604-613.

[23] Fox, C. and Zonneveld, P. *IT control objectives for Sarbanes-Oxley: The importance of IT in the design, implementation, and sustainability of internal control over disclosure and financial reporting*, Rolling Meadows, IL: Guidance document: Information Technology Governance Institute, 2004.

[24] Frost and Sullivan. The 2011 global information security workforce study, https://www.mediabuzz.com.sg/research-march-11/frost-sullivan-s-2011-isc-2-global-information-security-workforce-study-gisws, Nov 2016

[25] Gefen, D., Straub, D. W. and Boudreau, M. "Structural equation modeling and regression: guidelines for research practice," *Communications of the AIS* , Volume 4, Number 7, 2000, pp. 1-77.

[26] Gendron, Y., Bedard, J. and Gosselin, M. "Getting inside the black box: A field study of practices in "effective" audit committees," *Auditing: A Journal of Practice and Theory*, 2004 (Spring), pp. 153-171.

[27] GTAG. *Global technology audit guide (GTAG): Information technology controls, Global Technology Audit Guide*, Illinois USA: The Institute of Internal Auditors, 2005.

[28] Hair, J. F., Hult, G. T. M., Ringle, C. M. and Sarstedt, M. *A primer on partial least squares structural equations modeling (PLS-SEM)*, Thousand Oak: SAGE Publications, 2014.

[29] Hamaker, S. (2004). "Principles of IT governance," *Information System Control Journal*, Volume 2, pp. 47-50.

[30] Hao, X. and Rainsbury, E.A. "Analysis of disclosure of Internal control information from Chinese listed companies - Data from cross listing companies," Auckland Region Accounting (ARA)

Conference, 4 December 2011, Auckland, New Zealand.

[31] Hardy, G. "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges," *Information Security Technical Report II*, 2006, pp. 55-61.

[32] Henseler, J., Ringle, C. M. and Sinkovics, R. R. "The use of partial least squares path modeling in international marketing," *Advances in International Marketing*, Volume 20, 2009, pp. 277-320.

[33] Horton, T., Le Grand, C., Murray, W., Ozier, W. and Parker, D. "Information security management and assurance: a call to action for corporate governance," *The Institute of Internal Auditors*, 2000.

[34] Hu, X. "Thinking about the relative aspects on IT control of our enterprises," *Science and Technology Management Research*, Volume 30, Number 8, 2010.

[35] Huang, S.-M., Hung, W.-H., Yen, D. C., Chang, I. C. and Jiang, D. "Building the evaluation model of the IT general control for CPAs under enterprise risk management," *Decision Support Systems*, Volume 50, Number 4, 2011, pp. 692-701.

[36] Huang, S. and Ge, J. (2016). "Defects and countermeasures of Chinese listed company's internal control - based on 2012 ~ 2014 main board listed company data," *Caikuai Yuekan*, Volume 10, 2016, pp. 57-60.

[37] International Compliance Association. "What is compliance?", https://www.int-comp.org/careers/a-career-in-compliance/what-is-compliance/, June 2016.

[38] ISACA (2009). The risk IT framework: principles, process details, management guidelines, maturity models, Rolling Meadows.

[39] ITGI. "IT control objectives for Sarbanes–Oxley: The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting," *IT Governance Institute*, Rolling Meadows, 2004

[40] ITGI. "IT control objectives for Sarbanes-Oxley — the importance of IT in the design, implementation and sustainability of internal control over the financial reporting and disclosure," 2nd edition, 2006.

[41] Janvrin, D., Payne, E.A., Byrnes, P., Schneider, G.P. and Curtis, M.B. "The Updated COSO Internal Control—Integrated Framework: Recommendations and Opportunities for Future Research," *Journal of Information Systems*, Volume 26, Number 2, 2012, pp. 189-213.

[42] Jarvis, C. B., Mackenzie, S. B. and Pldsakoff, P. M. "A critical review of construct indicators and measurement model misspecification in marketing and consumer research," *Journal of Consumer Research*, Volume 30, Number 2, 2003, pp. 199-218.

[43] Ken, K. K. W. "Partial least squares structural equation modeling (PLS-SEM) techniques using Smart PLS," *Marketing Bulletin*, Volume 24: Technical Note 1, 2013

[44] Klamm, B. K. and Watson, M.W. "SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology," *Journal of Information Systems*, Volume 23, Number 2, 2009, pp. 1-23.

[45] Krstić, J. and Đorđević, M. "Internal control and enterprise risk management - from traditional to revised COSO model," *Economic Themes*, Volume 50, Number 2, 2012, pp. 151-166.

[46] Lainhart, J. V. "An IT assurance framework for the future," *Ohio CPA Journal*, Volume 60, Number 1, 2001, pp. 53-74.

[47] Li, B. and Wei, T. "Statistical analysis of defect information disclosure of internal control of main board listed companies," *Caikuai Yuekan*, Volume 29, 2015, pp. 74-79.

[48] Li, C., Peters, G. F., Richardson, V. J. and Watson, M.W., "The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports," *MIS Quarterly*, Volume 36, Number 1, 2012, pp. 179-203.

[49] Li, R. "Analysis of Internal Control Information Disclosure Situation," *Communication of Finance and Accounting*, Volume 26, 2013.

[50] Li, Y., Chen, C. and Yu, J. "Evidence to internal control evaluation report from 2011 - Problems and Improvement: Disclosure of internal control reviews for China's listed companies," *Accounting Research*, Volume 8, Number 9, 2013.

[51] Liu, G. *Research on Quality and Economic Consequences of Internal Control Self-assessment Report*, 2015a.

[52] Liu, J. "Disclosures of information and analysis of the internal control of listed companies," *Economic Research Guide*, Volume 25, 2015b, pp. 71-100.

[53] Liu, Z. and Liu, J. "The internal control under information technology environment," *Accounting Research*, Volume 12, 2001.

[54] Mehta, A. "An Approach toward Sarbanes-Oxley ITGC Risk Assessment," ISACA Journal, Volume 5, 2010.

[55] Meyer, N. D. "Systematic IS governance: An introduction," *Information System Management*, 2004 (Fall), pp. 23-34.

[56] Ministry of Finance, China. *China Auditing Standard No. 28- Information System Audit*, 2009.

[57] Molina, L. M., Llorens-Montes, F. J. and Ruiz-Moreno, A. "Relationship between quality management practices and knowledge transfer", *Journal of Operations Management*, Volume 25, Number 3, 2007, pp.: 682-701.

[58] NIST. *NISTIR 7298 Revision 2 - Glossary of Key Information Security Terms National Institute of Standards and Technology*, 2013.

[59] Norman, C. S., Payne, M. D. and Vendrzyk, V. P. "Assessing information technology general control risk an instructional case," *Issues in Accounting Education*, Volume 24, Number 1, 2009, pp. 63-76.

[60] Patilis, C. "Enhancing governance, risk and compliance at alternative investment management companies leveraging the roles of regulatory compliance and internal audit," *Journal of Securities Law, Regulation and Compliance*, Volume 1, Number 4, 2008, pp. 379-385.

[61] PCAOB. *Staff questions and answers on Auditing Standard No. 2 – Internal Control*, 2005

[62] Petter, S., Straub, D. W. and Rai, A. "Specifying formative constructs in IS research," *MIS Quarterly*, Volume 31, Number 4, 2007, pp. 623-656.

[63] Pirta, R. and Strazdina, R. "Assessing the need of information technology control environment establishment," *Information Technology and Management Science*, Volume 15, Number 1, 2012.

[64] Proctor, P. and Vignaly, J. "The security implications of Sarbanes–Oxley," *Symantec Enterprise Solutions Webcast*, 2004

[65] PwC. *Managing cyber risks in an interconnected world - key findings from the global state of information security survey*, 2015.

[66] Remenyi, D., Money, A. and Sherwood-Smith, M. *The effective measurement and management of IT costs and benefits*, Butterworth-Heinemann, Oxford, 2000

[67] Reynolds, G. W. Information technology for managers, 2 edition, Cengage Learning, 2016

[68] Rikhardsson, P., Best, P., Green, P. and Roseman, M. "Business process risk management, compliance and internal control: a research agenda," *Second Asia/Pacific Research Symposium on Accounting Information Systems university of Melbourne*, 2006.

[69] Rikhardsson, P., Rohde, C. and Rom, A. "Exploring enterprise systems and management control in the information society: developing a conceptual framework," 6th International Research Symposium on Accounting Information Systems, 10-11 December 2005, Las Vegas, USA.

[70] Ringle, C. M. Sarstedt, M. and Straub, D. W. "A critical look at the use of PLS-SEM in MIS Quarterly," *MIS Quarterly*, Volume 36, Number 1, 2012, pp. 3-14.

[71] Savic, A. "Managing IT-related operational risks," *Economic Analysis*, 53(176), 2008, pp. 88-109.

[72] Spremić, M., Bajgorić, N. and Turulja, L. "Implementation of IT governance standards and business continuity management in transition economies: the case of banking sector in Croatia and Bosnia-Herzegovina," *Ekonomska Istraživanja: Ananstveno-stručni časopis*, Volume 26, Number 1, 2013, pp. 83-202.

[73] Symantec. "IT risk management report - trends through 2006," Vol. 1, 2007 (Feb), http://eval.symantec.com/mktginfo/enterprise/other_resources/ent-it_risk_management_report_02-2007.en-us.pdf

[74] Symantec. "Internet Security Threat Report," Vol 21, 2016 (April), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[75] Wallace, L. and Lin, H. "Information security and Sarbanes-Oxley compliance: an exploratory study," *Journal of Information Systems*, Volume 25, Number 1, 2011, pp. 185-211.

[76] Walters, L. M. "A draft of an information systems security and control course," *Journal of Information Systems*, Volume 21, Number 1, 2007, pp. 123-148.

[77] Wei, L. "Sino-US comparison of the internal control disclosure of information," *M and D Forum*, 2011

[78] Weidenmier, M. L. and Ramamoorti, S. "Research opportunities in information technology and internal auditing," *Journal of Information Systems*, Volume 20, Number 1, 2006, pp. 205-219.

[79] Woods, M. (2009). "A contingency theory perspective on the risk management control system within Birmingham City Council," *Management Accounting Research*, Volume 20, Number 1, 2009, pp. 69-81.

[80] Wright, S. and Wright, A. M. "Information system assurance for enterprise resource planning systems: unique risk considerations," *Journal of Information Systems*, Volume 20, Number 1, 2002, pp. 205-219.

[81] Yan, H., Du, T. and Shao, Y.Q. "The current situation of information disclosure of internal control of China's listed companies," *Research on*

Economics and Management, Volume 37, Number 3, 2016.
[82] Yang, Q. "Enterprise IT management and control capacity-clear IT management capability framework," 2011.
[83] Yang, X. "A brand-new canto composed for academic research on internal control," *Accounting Research*, Volume 7, 2005.
[84] Yang, X. "The barriers internal control research faces and the solutions," *Accounting Research*, Volume 2, 2006.
[85] Zhou, G. "Study on enterprise internal control in the information environment," 2013.
[86] Zhou, Y. and Zhuang, M. "Exploring IT risk, internal control response and compliance," *Modern Management Science,* Volume 11, 2011, pp. 35-38.

AUTHOR BIOGRAPHIES

Wing Han Brenda Chan is an assistant professor in the Faculty of Business Administration, University of Macau. Her research and publications focus on IS management, IS project management, and IT application development.

Kin-Meng Sam is an assistant professor in the Faculty of Business Administration, University of Macau. He has published several conference and journal papers regarding online consumers' decision-making styles, e-marketing mix, ontology and user acceptance of IT. His current interests include i) e-marketing mix, ii) ontology-based business system, iii) online consumer behavior, iv) user acceptance of IT and, iv) text-mining system.

Dan Liu has nine years of experience in various fields such as financial assurance and audit, financial advisory and internal audit. She was Assistant Audit Manager at Sands China Limited. She has also worked at KPMG China. She holds the CIA certificate.

APPENDIX A

Three main constructs of research

Construct	Indicator Type	Items	Source or Basis
ITGC	Formative-2nd order		(ITGI, 2006) (Chan and Lao, 2009)
IT control environment	Formative-1st order	-IT governance process (information systems strategic plan, IT risk management process, compliance and regulatory management, IT policies, procedures and standards) -Monitoring -Reporting	(ITGI, 2006)
Access to programs and data	Formative-1st order	-Unauthorized access: adequate access control activities, such as secure passwords, internet firewalls, data encryption and cryptographic keys -User accounts and related access privilege controls	(ITGI, 2006) (Chan and Lao, 2009)
Program development	Formative-1st order	Acquisition and implementation of new applications: e.g., System development and quality assurance supports identification of automated solutions, system design and implementation, documentation requirements, testing, approvals, project management and oversight requirements, and project risk assessment	(ITGI, 2006) (Chan and Lao, 2009)
Program change	Formative-1st order	Controls involve required authorization change request, review of changes, approvals, documentation, testing and assessment of changes on other IT components and implementation protocols	(ITGI, 2006) (Chan and Lao, 2009)

Construct	Indicator Type	Items	Source or Basis
Computer operations	Formative-1st order	-Ongoing controls on daily delivery of information service: service level management, management of 3rd party services, system availability, customer relationship management, configuration and system management, problem and incident management, operation management scheduling and facilities management -Controls over effective acquisition, implementation, configuration and maintenance of operating system software, database management systems, middleware software, communications software, security software and utilities that fun the system and allow applications to function	(ITGI, 2006) (Chan and Lao, 2009)
Compliance	Formative-2nd order		(Symantec, 2007)
Data Retention	Formative-1st order	Securing confidentiality of private and personal information	(Symantec, 2007)
Data Protection	Formative-1st order	Ensuring data is stored securely and retained for access by legitimate users	(Symantec, 2007)
Corporate Governance	Formative-1st order	Assuring the public disclosures accurately reflect corporate performance	(Symantec, 2007)
Intellectual Property	Formative-1st order	Protecting corporate intellectual property	(Symantec, 2007)
Civil, Criminal and legal framework	Formative-1st order	Assuring the IT systems and networks system support legal infrastructure	(Symantec, 2007)
National Security	Formative-1st order	Protecting citizen and national infrastructure from terrorism, war, or national disaster	(Symantec, 2007)
IT-related Risk	Formative-2nd order		(ISACA, 2009)
Security risk:	Formative-1st order	Corruption of information, External fraud, Theft of financial assets, Damage to reputation and brand, Damage to assets	(Symantec, 2007)
Availability risk:	Formative-1st order	Abandoned transactions and lost sales, Reduced customer, partner, employee confidence, Interruption or delay of business critical processes, Reduce IT staff productivity	(Symantec, 2007)
Performance risk:	Formative-1st order	Reduced client satisfaction, Reduced client or partner loyalty, Reduced user productivity, Interruption or delay of business critical process, Lost IT productivity	(Symantec, 2007)
Compliance risk:	Formative-1st order	Damage to reputation, Breach of client confidentiality, Litigation, Executive productivity	(Symantec, 2007)

APPENDIX B

Outer-weights of formative indicator/dimension

Indicators	Outer-weights	*t* statistics	Indicators	Outer-weights	*t* statistics
ITCE_1 -> ITCE	0.362	1.920	COMP_1 -> COMP	0.275	2.898
ITCE_2 -> ITCE	0.085	0.498	COMP_2 -> COMP	0.287	2.466
ITCE_3 -> ITCE	0.074	0.621	COMP_3 -> COMP	0.033	0.327
ITCE_4 -> ITCE	0.086	0.724	COMP_4 -> COMP	0.156	1.348
ITCE_5 -> ITCE	0.543	4.649	COMP_5 -> COMP	0.293	2.930
APD_1 -> APD	0.439	2.659	COMP_6 -> COMP	0.158	1.914
APD_2 -> APD	0.619	3.949	AR_1 -> AR	0.623	5.619
PC_1 -> PC	0.412	5.357	AR_2 -> AR	0.468	3.906
PC_2 -> PC	0.220	2.444	CR_1 -> CR	0.836	5.568
PC_3 -> PC	0.461	6.383	CR_2 -> CR	0.210	1.219
PD_1 -> PD	0.553	3.927	PR_1 -> PR	0.714	6.428
PD_2 -> PD	0.485	3.329	PR_2 -> PR	0.335	2.763
CO_1 -> CO	0.655	6.612	SR_1 -> SR	0.613	5.404
CO_2 -> CO	0.417	4.001	SR_2 -> SR	0.449	3.786