國立台灣大學管理學院資訊管理研究所

碩士論文

Department of Information Management

College of Management

National Taiwan University

Master Thesis

ISO 27001 之採用

– 整合創新擴散及制度理論之角度

ISO 27001 Adoption

– Integrating Innovation Diffusion and Institutional Theories

鍾振杰

Chen-Chieh Chung

指導教授：許瑋元 博士

Advisor: Wei-Yuan Hsu, Ph.D.

中華民國九十九年七月

July, 2010

國立臺灣大學碩士學位論文
口試委員會審定書

ISO 27001 Adoption

- Integrating Innovation Diffusion and Institutional Theories

本論文係 鍾振杰 君（學號 R97725048）在國立臺灣大學資訊管理學系、所完成之碩士學位論文，於民國九十九年七月二日承下列考試委員審查通過及口試及格，特此證明

口試委員：許瑋元

王大維

張欣綠

所　　長：陳靜枝

致謝

本篇論文的完成，首先要誠摯的感謝指導教授許瑋元博士，老師悉心的教導與指引，使我在這兩年中獲益匪淺。老師對於專業知識之淵博、思路邏輯之清晰、以及待人處事之態度，都是我在這二年以及未來當中，一個學習的典範。而在論文口試期間，承蒙張欣綠教授及王大維教授的指正並惠賜寶貴的意見及建議，使本論文能夠更加的完備，在此致上最誠摯的感謝。本論文的完成另外亦得感謝勤業眾信的 Sarah 學姐的協助，為我們找了業界專家來檢閱我們的問卷並提供諸多的建議，使得我們的問卷更加清楚易懂。

感謝Shirley、育滋學姐們不厭其煩的為我解答研究上的疑問並提供建議以及想法，且不斷的鼓勵與激勵我們，使得許多研究上的疑難能夠迎刃而解。也感謝實驗室的同學禹帆、偉銘、建宇，由於有你們，讓研究所生活增添許多色彩與樂趣，並且讓我了解到許多做事與做人的道理。還有小開、似琪、其其，都是共同學習與分享的好伙伴，也希望未來能夠有機會與大家共事。還有女友以潔在背後的支持與陪伴更是我前進的動力，謝謝你在這二年陪伴我走過，並且也謝謝你在我研究與寫作的過程當中忙錄的時候，展現的體諒與包容。以及這一路上所有幫助與指點過我的人，沒有你們，也不會有今天的我，謝謝！

最後，謹以此文獻給我摯愛的家人，感謝我的家人多年來的支持與栽培。

鍾振杰謹致

國立台灣大學資訊管理研究所

中華民國九十九年七月

摘要

近年來，由於資訊安全事件對於組織的衝擊，使得資訊安全對於組織而言，其重要性不斷的攀升。改善其資訊安全的控制及管理，對於各種組織來說都是致關重要的。而在資訊安全管理領域當中，對於組織欲強化其資訊安全管理，ISO 27001 一直扮演著重要的角色，然而在過去的文獻當中，對於 ISO 27001 的研究卻非常有限，而且幾乎沒有任何學術針對 ISO 27001 採用意圖作一深入的研究。因此我們結合了兩個過去經常被使用來研究採用意圖的重要理論，即創新擴散理論及制度理論，來發展我們的研究模型，並且收集了 52 個台灣的組織的資料來驗證此一模型。分析結果顯示 ISO 27001 的複雜性及台灣制度環境上的壓力，對於組織採用 ISO 27001 意圖的高低，具有顯著的影響力。本研究結果為學術上缺乏對於 ISO 27001 採用意圖的研究，做了一部分的補充，並且可以提供實務上組織在採用 ISO 27001 時的一個參考。此外，本研究亦使創新擴散理論及制度理論的文獻進一步延伸至資訊安全管理此一領域。

關鍵字：ISO 27001、資訊安全管理系統、採用意圖、管理創新、創新擴散理論、制度理論。

Abstract

Since the importance of information security and its severe impacts on organizations, the improvements of information security controls as well as managements are crucial for all organizations. For the information security management, ISO 27001 is the most important standards and it plays an important role while the organizations are considering strengthening their security management. However, there are scanty of academic researches focus on the ISO 27001 issues and nearly no researches were studying the adoption intentions of ISO 27001. Therefore we develop the research model from two theories, and the hypothesized research model is tested using empirically data collect from 52 organizations in Taiwan. The results suggest that complexity and institutional influences have a strong impact on the adoption intention of ISO 27001. This study provides several implications on both academic and practical. It also extended the empirical literature of institutional and innovation diffusion studies to the area of information security.

Keywords: ISO 27001, Information Security Management System, Adoption Intention, Administrative Innovation, Diffusion of Innovation Theory, Institutional Theory.

Table of Contents

List of Tables

List of Figures

Chapter 1 Research Issues

1.1 Motivation and the Scope of the Research

Digitalized information has become the new currency of business; it crosses any kind of boundaries, national, organizational, or geographical boundaries. The use of the information is a necessity for a corporation to do daily operations and business. Without appropriate information, neither the managers can make decisions correctly nor can the employees do any transactions or affairs. Hence, information is critical assets for corporations, but increasing uses of information result in higher risk. It should be well stored, transmitted, and protected, and only be used by authorized people or organizations. As the information security study of DTI/PWC (2008) states:

> *"Information is the new currency of business – a critical corporate asset whose value rises and falls at different times, and in different ways, depending on when, how, where and by whom it is placed into circulation as a medium of exchange. Therein lie the risks. And the opportunities."* (DTI/PWC, 2008)

Information as a new currency has two meanings, one is that it has its value, and another is that currency is a flow transmitting between corporations. Hence, a corporation faces many information security risks, once information incidents occur, it not only causes financial loss, e.g. maintenance or recovery fee for servers or data, but also damages the intangible assets, such as business secret, confidential data, reputation of their corporation, or trust of their partners and clients. For any kind of organizations, the security incidents could possibly lead to severe problems, and they should strive for averting such problems.

Another reason for a corporation to build an information security system is the compliance for the laws and regulations. The regulatory bodies compel the corporations to take some actions to improve their information security. For the relating laws and regulations, Whitman and Mattord (2008) summarized some important laws and regulations, and we rearranged that into table 1-1. Among those laws and regulations, the most important are Sarbanes-Oxley Act and Basel II for information security managements.

Table 1-1: Key U.S. Laws Related to Information Security

Act	Subject	Descriptions
Communications Act of 1934, (amended 1996 and 2001)	Telecommunication	Regulates interstate and foreign telecommunications
Computer Fraud and Abuse Act, (amended 1994, 1996, and 2001)	Threats to computers	Defines and formalizes laws to counter threats from computer-related acts and offenses
Computer Security Act of 1987	Federal Agency Information Security	Requires all federal Computer systems that contain classified information to have surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Economic Espionage Act of 1996	Trade secrets	Designed to prevent abuse of information gained by an individual working in one company and employed by another
Federal Privacy Act of 1974	Privacy	Governs federal agency use of personal information
Gramm-Leach-Bliley Act of 1999(GLB) or Financial Services Modernization Act	Banking	Focuses on Facilitating affiliation among banks, insurance, and securities firms; it has significant impact on the privacy of personal information used by these industries
Health Insurance Portability and Accountability Act (HIPPA)	Health care privacy	Regulates collection, storage, and transmission of sensitive personal health care information
Sarbanes-Oxley Act of 2002	Financial Reporting	Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting

Security and Freedom Through Encryption Act of 1999	Use and sale of software that uses or enables encryption	Clarifies use of encryption for people in the USA and permits all persons in the U.S. to buy or sell any encryption product and state that the government cannot require the use of any kind of key escrow system for encryption products
USA PATRIOT improvement and reauthorization Act 2006	Terrorism	Made permanent 14 of the 16 expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity
Basel II Accord	Banking	Create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

Source: rearranged from (Whitman & Mattord, 2008) pp.93-94.

Sarbanes-Oxley Act

Sarbanes-Oxley Act (SOX), a regulation signed into US law in response to the Enron, WorldCom, Tyco, and other scandals, is a critical piece of legislation that affects the executive management of publicly traded organizations and accounting firms. The main purpose of the regulation is to prevent financial fraud and deception. It contains eleven titles that describe specific mandates and requirements for financial reporting and each title consists of several sections. One of the most important parts of SOX is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting. The adequacy of controls depends substantially on mainstream issues for information security professionals (Schultz, 2004). The financial information is stored in hardware, processed by computing systems, and transferred by computing networks. All of those hardware, systems, and networks require certain adequate authentication and access controls. As stated by Schultz, "information security has accumulated a large body of knowledge and technology that addresses all of these issues" (Schultz, 2004), the SOX regulates organizations to comply with it and obliges them to improve their controls and managements with information security.

Basel II Accord

Basel II Accord creates regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. Basel II additionally requires capital provision for operational risks, which was defined by the Basel II Committee as “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events”. There are three approaches, Basic Indicator Approach, Standardized Approach and Advanced Measurement Approach, available for calculating amount of capital required to cover risk. Basel II elaborates “Loss Event Type Classification (operational risk)” (Basel, 2004), and those type categories (level 1) are (1) Internal fraud, (2) External fraud, (3) Employment practices and workplace safety, (4) Clients, products and business practices, (5) Damage to physical assets, (6) Business disruption and system failures, and (7) Execution, delivery and process management. Under each level 1 categories, there are level 2 categories and activities (level 3), such as unauthorized activity, theft and fraud, and others. These categories are highly related to information security and risk management, and therefore banks can acquire knowledge from the two areas.

A corporation has to confront these laws and issues, and improve their information security to protect its asset, maintain its good reputation, and comply with laws and regulations (E&Y, 2008). The consequences are that they have to introduce information security related controls, policy, and standards into their organizations. The percentage of information security budget increasing steadily in IT budget (Richardson, 2008) shows that information security is becoming more and more important and receiving more attentions.

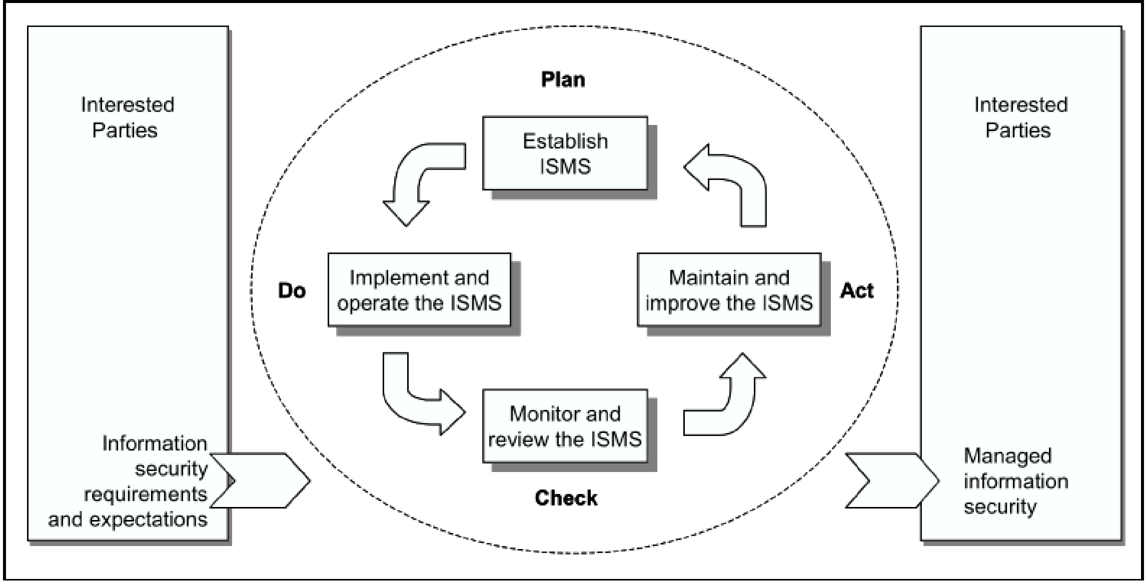
In the past few decades, almost all approaches for information security are “technical solutions”. However, in recent years, people realized the importance and effectiveness of managerial solutions, i.e. the effectiveness of information security policy, information risk assessment, and employees’ security awareness trainings. Combining technical and managerial solutions can make the corporation be more secure. For example, with information security standards and policies, technicians could select suitable technologies products for the organization and employees could have a clearer view of their responsibilities and accountabilities.

The question is, with so many information security technical and managerial issues, how does an organization know what to do, how to improve their information security, or how should they let the others know they are doing well? One of the answers is certification, which ensures the organization complied with a specific standard that guarantees a minimum quality. An information security management standard, e.g. ISO 27001, involves many aspects of security, such as policy, environments, personnel, and technologies. The standard provides a framework to help organizations known how to improve their information security. Once an organization establishes a management system that meets the ISO 27001 requirements and applies for the certification, an external registrar would visit the firm to audit and analyze the system and its security features. If the system meets the standards, the registrar will issue an official certificate that states that the ISMS meets the ISO27001 requirements. An organization must meet each requirements of the standard to get certified, and that means if we believe in the convincible authorities (e.g. ISO and BSI) which grant the certification, we can trust the organization with certification is doing information security well. .

ISO/IEC 27001:2005

In 2005, the International Organization for Standardization (ISO) published ISO/IEC 27001:2005 *(Information technology - Security techniques - Information security management systems – Requirements)*, which is a revised and updated version of British Standard BS7799 part2. ISO 27001 provides a model and promotes process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) which consists many aspect of information security, such as security policy, asset managment, human resource security, physical and environmental security, communications and operations management, access control, etc. The process approach highlights the importance of (1) understanding an organization's information security requirements and the need to establish policy and objectives for information security; (2) implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks; (3) monitoring and reviewing the performance and effectiveness of the ISMS; and (4) continual improvement based on objective measurement (Fenz, et al., 2007; ISO, 2005a). It is built on the Plan-Do-Check-Act (PDCA) process model (see figure 1-1).

Figure 1-1: PDCA Model Applied to ISMS Processes


Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security

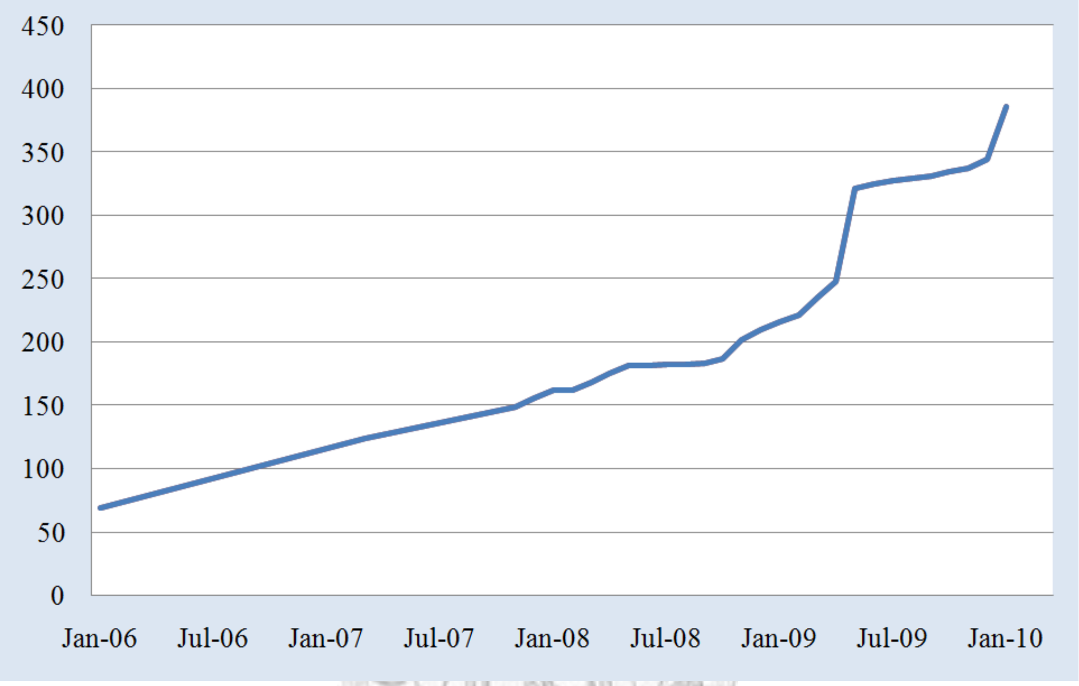
Source: ISO 27001 standard (ISO, 2005a)

From the above, we can understand why information security issues are crucial, and how certification can help the organizations to improve their information security management and reduce the impact of information security incidents. In the global, there are 6443 certificates registered to "International Register of ISMS Certificates[1]" until May 2010 (Version 199). In Taiwan, the number of certificates shown in the websites is 373 (version 199, May 2010), and the growth of past several years was shown in figure 1-2. In the recent years, the number of certificates of Taiwan has been increasing sharply. Especially in 2009, more than one hundred organizations got the certifications in this year in response to "Government Agencies Information Security Level of Responsibilities Classification Program[2]", since the year 2009 is the deadline for the class A agencies[3] to get certified. Such a phenomenon drew our attention, why did so many organizations decide to adopt ISO 27001? Are there any unusual reasons behind the organizations that

[1] Website: http://www.iso27001certificates.com/
[2] 政府機關資訊安全責任等級分級作業施行計畫
[3] The class A agencies are the most important kernels of the government operations, therefore such agencies have highest priority. For detail information, please see the official documents

lead to such states?

Figure 1-2: Number of Certificates in Taiwan



Source: International Register of ISMS Certificates

Actually, in the past years, there were some organizations that adopted and implemented an information security management system but some did not. What are the differences between them? What really drives an organization to adopt an information security system? Most of the researches focus on the effectiveness of implementation, whereas little researches discussed the reasons why an organization decided to adopt it. The gap should be addressed, so this research expects to find out the reasons why an organization decided to adopt ISMS, more specifically, ISO 27001.

1.2 Research Question and Objectives

In this research, our main questions are “What are the reasons an organization decide to adopt ISMS?” To answer this question, we have to discuss the essence of ISMS and its characteristics that lead to the adoption decision. Besides, we also have to discuss the environments of Taiwan that possibly influence the decision.

Hence, our research objectives are (1)”What is ISMS? What is the essence of ISMS?”, (2)”What are the characteristics of ISMS that drive an organization decide to adopt ISMS?”, and (3)“What are the institutional pressures that an organization may face while considering information security standards?”

We regard ISMS as an administrative innovation and identify the possible drivers from two theories (i.e. diffusion of innovation and institutional theory) that make an organization decide to adopt such an administrative innovation. By analyzing the empirical data collecting from organizations in Taiwan, we expect to find out the motivations behind these organizations that adopted ISO 27001.

1.3 Structure of the Thesis

This thesis is organized as follows. Chapter 1 provides overview information on the current information security issues and the motivation of this research. In that chapter, we also form our main research questions and objectives. Chapter 2 covers the literatures review, which reflects the information security literature and the gap in current researches, especially the limited in information security management researches and the lack of research focusing on ISO 27001 adoptions. And in chapter 3, we will discuss the ideas of administrative innovation and two important theories while studying the adoption intention (i.e. diffusion of innovations and institutional theory). The proposed research framework integrating the two theories is also presented in chapter 3. The chapter 4 included the measures of independent and dependent variables that discussed in chapter 3, and also discussed several control variables that might influence the adoption decision. The sampling plan and the research methodologies that used to test the model and hypotheses also introduced in chapter 4. The model building and hypotheses testing using structural equation modeling (SEM) were presented in chapter 5, and the relating discussion also included in this chapter. The final chapter, chapter 6, concluded our research and provided several limitations of this research and directions for future research.

Chapter 2 Literature Review

The term “Information security (InfoSec)” means protecting information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities (ISO, 2005b). This description points out the multifaceted nature of information security. For example, Siponen and Oinas-Kukkonen (2007) reviewed the research on information security up to early 2000 and identify four security issues (i.e. access to information systems, secure communication, security management, and development of secure information systems). D'Arcy and Hovav (2008) provided an integrative framework for studying information security management research and the framework contains five dimensions: (1) financial and economic impact, (2) strategy and best practice, (3) behavioral issues, (4) standards and regulations, and (5) security technology. Therefore, information security involves multiple aspects and it could not be explained by one single dimension.

Since the rise of information security management (ISM) (D'Arcy & Hovav, 2008; von Solms, 2000), in the following section, we reviewed and classified the literature between 1995-2009 (We also covered some 2010 issues of several journals, and several journals’ first publication was published after 1995, hence the coverage of such journals was from its first publication to 2009 or 2010. For the detail survey period of each journal, please see appendix A) on information security into two dimensions: *technology* and *management*. There conceivably exists some researches that could not be mapped into the two dimensions, but our purpose here is to know current development of information security rather than intending to classify the existing researches exhaustively.

Since the existing classification schemas reflect a limited computer science perception of security research (Siponen & Willison, 2007), we use the items in

ISO27002(ISO, 2005b) as well as the findings in Siponen and Willison (2007) as a guideline to classify existing researches, and we also refer some information security related handbooks[4] to make the classification be more exhaustive.

We surveyed a total of 1990 IS security related articles published in nine widely-known MIS journals and three security journals of the period 1995-2009. The MIS journals that we surveyed are: MIS Quarterly (MISQ), Information Systems Research (ISR), Information Systems Journal (ISJ), Information & Management (I&M), Journal of Information systems (JIS), European Journal of Information Systems (EJIS), Journal of Management Information systems (JMIS), Communications of the Association for Information Systems (CAIS), Journal of the Association for Information Systems (JAIS), and security journals are: Computers & Security, Information Security Journal , Information Management & Computer Security.

2.1 Information Security Technologies

In the technology dimension, we identified 5 main categories; they are “Cryptography and Secure Communications”, “System, Software, and Data Security”, “Security Attacks and Malwares”, “Physical Security”, and “Technological Standards and Certifications”. The search results show that 1233 out of 1990 researches are technologies related articles (see table 2-1 and appendix A for details).

[4] The handbooks including Computer and information security handbook (Vacca, 2009), Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions (Knapp, 2009), Handbook of Information Security Volume 1-3 (Bidgoli, 2006), Handbook of Research on Information Security and Assurance(Gupta & Sharma, 2008), Information Security Management Handbook (Tipton & Krause, 2007), and Social and Human Elements of Information Security: Emerging Trends and Countermeasures (Gupta & Sharman, 2009)

Table 2-1: Categories of Information Security Technologies and Researches in 1995-2009

Category	Subjects	IS Security	IS
Cryptography and Secure Communications	Cryptography, Public key infrastructure (PKI), Digital signatures, Digital payment, Key management, Secure communications, Wireless security, Identification & authentication, and Access control.	558	5
System, Software, and Data Security	Systems security, Firewalls, Intrusion detection systems, Code security, Secure voting issues, Secure systems design, Database security, and Applications security.	315	9
Security Attacks and Malwares	System attacks, Types of security attacks, Hackers and Hacking, Computer crime, Viruses and malware, Spam, Cryptanalysis, and Information warfare.	275	6
Physical Security	Physical security, Hardware security, Workstation security, Personal security, PC security, and Biometric authentication.	70	3
Technological Standards and Certifications	Technical standards, Technical certifications, and IT Security Evaluation.	15	1
Total		**1233**	**24**

Cryptography and Secure Communications

The first category is “Cryptography and Secure Communications”, including cryptography, public key infrastructure (PKI), digital signatures, digital payment, key management, secure communications, and wireless security. All the subjects in this category involve encryption/decryption methods and its management.

The recent developments of cryptography methods include “quantum cryptography” and “elliptic curve cryptosystem”, and earlier methods, such as RSA, DES, AES, and Whirlpool. The recent researchers apply cryptosystem in different situation and improve the effectiveness and efficiency. Chen et al. (2003) used the elliptic curve cryptosystem to improve the efficiency of proxy multi-signature schemes, which was introduced by (Mambo, et al., 1996). Harn and Ren (2006) proposed an efficient RSA multi-signature scheme that has constant signature length and verification time, and the scheme is secure against forgery under chosen-message attack.

System, Software, and Data Security

Second category is "System, Software, and Data Security". It contains the security issues related to systems and software, such as various systems and applications security, code security, secure systems design, and database security. Those researches focus on security design and coding of systems, software and applications fall in this category, since they all consider security from the programming perspective and seek to improve its security.

Wang and Wang (2003) addressed software security threats and risks through McCall's framework of software quality factors and divided the threats and risks into three categories (i.e. Application layer, Platform layer, and Network layer) based on the attack target. Tsipenyuk et al. (2005) also identified and taxonomize the software security errors to help developers avoid making these mistakes.

Security Attacks and Malwares

The category of "Security Attacks and Malwares" includes the systems vulnerabilities attacking and hacking methods, viruses and malwares, spam, cryptanalysis, and computer crimes. Although attacking and hacking are opposite to systems and software protection, understanding and researching on these methods are beneficial for designing a better system that can deal with the malicious attacks.

There are still some problems that cannot be solved efficiently. Distributed Denial of

Service (DDoS), for instance, remains a great threat to Internet though various approaches and systems have been proposed (Gupta, et al., 2009; Li, 2006). In their recent work, Xu and Lee (2003) isolate and protect web servers against DDoS attacks. They address the attack and countermeasure issue by using a game-theoretic framework that configures the server in the way that provides the best service possible while under attack.

Physical Security

The physical security issues belong to the category of "Physical Security", such as hardware, workstation, PC, personal security, and biometric authentication. If someone could break in the computer/server room and steal the hardware, hard drives, for instance, they could bypass other security controls and get the confidential data easily. Therefore, physical security is as important as other security issues for protecting data from various threats.

Physical security also includes the fire control, surveillance systems, uninterruptible power supply, and other equipments that could prevent the hardware and people from being physically damaged or lost. Weingart (2000) describes some known physical attacks and the defense mechanisms that can be useful in deterring or detecting the attacking methods.

Biometrics, described as the science of recognizing an individual based on human physical traits, is widely accepted as a legitimate method for determining an individual's identity, and its systems have been adopted in many applications as a means to establish identity. Jain et al. (2006) discussed some issues that need to be addressed for making biometric technologies an effective tool for providing information security.

Technological Standards and Certifications

The IT security standards and certifications, such as Trusted Computer System Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC), and other standards, fall into this category, but excluding the managerial standards or certifications. IT Security Evaluation started and predominated by the US DoD TCSEC, and overtaken by European criteria ITSEC. Afterwards, the Common Criteria originated out of three standards, including above two standards and one Canadian standard followed from the US DoD standard called "Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)", and was enshrined an international standard (ISO/IEC 15408) in 1999 (Fischer, 2007).

Tierney (2008) applied Common Criteria in smart card application, Mellado et al. (2007) presented a Common Criteria centred and reuse-based process that deals with security requirements at the early stages of software development.

2.2 Information Security Management

We also identified 7 main categories of information security management and there are 757 articles (see table 2-2 and appendix A for details).

Table 2-2: Categories of Information Security Management and Researches in 1995-2009

Categories	Subjects	IS Security	IS
Risk Management	Risk management, Risk assessment, Risk treatment, Risk monitoring and review, and Risk analysis	80	18
Awareness, Behavior, and Education Issues	Security awareness, Security education & training, Security behavior, and Culture	87	5
Legal and Ethical Issues	Copyright & piracy issues, Security and privacy, Security and ethics, Compliance, and other legal aspects of security	100	32
Security Management Plan, Policies, Governance, Standards, and Certifications	Security management and plan, Policies, Governance, Security management standards and Certifications	150	12
Business Continuity Planning and Management	Business continuity planning and Disaster recovery	35	6
Security Investment and Strategy	Info security expenditure, Security economics, Strategy, and Competitive advantages	27	8
Audit and Assurance	Computer audit, Information systems audit and Information assurance	11	7
Total		**757**	**88**

Risk Management

The process of information security risk management defined in (ISO, 2008) consists of risk assessment, analysis, identification, estimation, evaluation, treatment, monitoring, review, communication, and acceptance. The researches focus on risk management activities and methodologies are fall into this category.

For the information security management, how to manage information risk is a vital issue (Blakley, et al., 2001; Bodin, et al., 2008), and risk management plays a major role in accessing and treating the information security risks to a acceptable level. As (ISO,

2008) wrote, "*A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS).*" By using the risk management approach, the limited resources allocation can be determined and justified to security needs, and the impact of certain security incidents can be reduced to as lower as possible under such risk and cost trade-off situation. Apart from (ISO, 2008), Stoneburner et al. (2002) provide guidelines that describe the risk management methodology, how it fits into each phase of the SDLC, and how the risk management process is tied to the process of system authorization.

The current developments of risk management in the information security area include searching for appropriate methodologies for the risk analysis in different circumstances (Smith & Eloff, 2002; Sun, et al., 2006). Sumner (2009) provided a methodology based upon an analysis of perceived impact and probability of occurrence of information security threats.

Awareness, Behavior, or Education Issues

The users' information security awareness and behavior is crucial, as information security control techniques or procedures could be misused or misinterpreted, and thereby losing their real usefulness. The ways to raise users' awareness and correct their behavior are by using security education and training, and eventually, security became part of the organization's culture. The awareness, behavior, education, training, and culture issues of security belong to this category.

To accomplish the goal that security becomes a part of organization's culture is arduous. The current researches aim to better understand users' behaviors and the reasons behind their acts, and thus develop a more suitable training program or deterrence methods. Dinev et al. (2008) examined user behavior towards protective information technologies across different cultures and suggested that, while the multiple cultures coexist, the cultural factors should be deliberated. D'Arcy et al. (2009) combined works from criminology, social psychology, and information systems to form an extended deterrence theory model, which was empirically tested, and the results suggest that three practices (i.e. user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring) can deter IS misuses.

Legal and Ethical Issues

There are many legal aspects of information security. For the intellectual property publishers (e.g. software, music, and books), the copyright and piracy are important concerns; for the e-commerce, online transaction, and healthcare companies, protecting their customers' personal information (i.e. privacy) is crucial. Therefore, for these companies, they need to keep the systems which stored the information assets from being compromised. These legal issues, including the compliance and ethics topics, are categorized as “Legal and Ethical Issues”.

In the subject of copyright and piracy, Gopal and Sanders (1997) found that individuals are deterred from software piracy if the policy state and warn of the legal consequences, and resulted in lower piracy intentions. Moreover, Straub (1990) also conclude that the deterrence measures are a useful strategy for reducing computer abuse activities (e.g. illegally copy and sell software). For the privacy and ethical issues, Culnan and Williams (2009) illustrate their arguments that organizations have a moral responsibility to individuals to avoid causing harm and to take reasonable precautions.

Security Management Plan, Policies, Governance, Standards, and Certifications

While planning and implementation of security management, such as implement an

ISMS, the organization should opt for a combination of many aspects (e.g. policies, standards, technology, human issues, legal and ethical issues) in establishing an ISMS Eloff and Eloff (2003). The planning of security management, security policies developments, governance, and other planning and implementing issues should be addressed during the implementation process, and it require the overall corporate involvements. von Solms and von Solms. (2004) identified 10 essential aspects that should be taken into consideration during the information security governance plan.

Business Continuity Planning and Management

Business continuity issues, after a devastating event 911, receive much more attentions. Not only the natural disasters (e.g. flood, earthquakes, and hurricanes) can be the causes of the physical damage of buildings, crash of mainframes, and death of people, but the human kind (e.g. terrorism attacks) could be a great threat that results in these catastrophic consequences. Except the calamities above, business interruption could be caused from other events, such as human error, utility disruptions, and malicious threats. How can a company recovered from the business interruption rapidly is critical to a company's survival as a going concern.

Cerullo and Cerullo (2004) propose guidelines for developing and improving a firm's BCP, which has three components (i.e. business impact analysis, disaster contingency and recovery plan, and training and testing component). Gibb and Buchanan (2006) combined various authors proposed different development cycles for BCM into a framework for BCM program, which consist of multiple phases, including program initiation, risk analysis, monitoring and control, implementation, education and training, etc.

Security Investment and Strategy

With billions of dollars being spent on information security related products and services each year, the economics of information security investment has become an important area of research, with significant implications for management practices. How much investment is enough, what kind of risk level is acceptable, and which strategy should be taken under the cost and benefits trade-off? In the speedy and competitive age, the decisions that an organization made have to be measured its benefits by any means, so do the security investment decisions.

Cavusoglu et al. (2005) proposed a comprehensive model to analyze IT security investment problems that overcome some of the limitations of risk analysis and cost effectiveness analysis methods. Gordon and Loeb (2002) presented an economic model that take into account the vulnerability and potential loss of a breach to determine the optimal amount that should invest to protect a given set of information.

Audit and Assurance

Information systems audit, as known as information technology audit or computer audit, is a process to ensure the information systems are safeguarding assets, maintaining data integrity, and operating effectively. The IS audit process consists of examining the controls within an information system, collecting the evidence of an organization's information systems, practices, and operations, and evaluating the data and operations processed by the systems.

2.3 Implications for current status of information security research

From the search results discussed earlier, we can find that (1) in the past years, the information security research are neglected in MIS journals, and (2) even in information security journals, most of the recent researches focus on the aspect of technologies rather than management, the percentage of management aspect is relatively small. Besides, the current keyword classifications, provided by ACM, IEEE, ISR and MISQ, contain few items related to information security and are technical oriented (Siponen & Willison, 2007). This shows the social or management topics received less attention relative to technical. Since the need for understanding the social and management aspects as well as technical aspects (D'Arcy & Hovav, 2008; Dhillon & Backhouse, 2001; Siponen & Willison, 2007), current states of information security needs more social and management related efforts. Moreover, most of current papers were subjective argumentative rather than empirical test, and this may fail to provide a firm basis for future research (Siponen & Willison, 2007).

Back to our research interests, we also surveyed the ISO 27001 (as well as ISO 17799 and BS7799) related studies published in the past 15 years and found only 16 articles used ISO 27001, ISO 17799, or BS7799 in their keywords or abstracts. Besides, no research inquired into the intentions of adopting 27001. Hence, Our research question, the reason why so many organizations are willing to adopt ISO 27001, still remain unsolved after searching from the literature. In view of the importance of ISO 27001, the lack of academic researches aiming to ISO 27001 adoption intentions ought to be addressed.

In the following chapters, we will examine the attributes of ISO 27001 and find the suitable theories to help us develop the model. After developing the model, we select the methodologies to analyze the adoption intention using the sample we collected from organizations in Taiwan.

Chapter 3 Research Framework

3.1 Administrative Innovation

Innovation, in the past decades, has been studied from several perspective, such as adoption of innovations (Damanpour, 1992; Kimberly & Evanisko, 1981), diffusion of innovations (Rogers, 1995), and innovations at different levels of analysis. Innovation is generally defined as “any idea, practice or material artifact perceived to be new by the relevant unit of adoption” (Westphal, et al., 1997). Since our research focus on the adoption intention of innovation, we take Damanpour's (1992) definition of innovation, e.g. “the adoption of an idea or behavior, whether a system, policy, program, device, process, product or service, that is new to the adopting organization”.

It has been argued that distinguishing types of innovation is necessary for understanding organizations' adoption behavior and identifying the determinants of innovation in them (Damanpour, 1991; Downs Jr & Mohr, 1976; Knight, 1967; Rowe & Boise, 1974). Among the three typologies of innovation (i.e. administrative and technical, product and process, and radical and incremental), the administrative and technical innovation typology gained the popularity (Damanpour, 1991), and it's suitable for this research since the characteristics of information security management. *Administrative innovation*s involve organizational structure and administrative processes, which are not directly related to the basic work activities but directly relate to its management (Damanpour, 1991; Kimberly & Evanisko, 1981; Knight, 1967). On the other hand, *Technical innovations* pertain to products, services, and production process technology, which are related to basic work activities and can concern either product or process (Damanpour, 1991; Kimberly & Evanisko, 1981; Knight, 1967).

As Hsu et al. (2010) noted that technical innovation of IS security deals with security technology artefact and administrative innovation refers to "a philosophy of developing a security management program including the security policy, management committee, team structure and employee education". Hsu et al. (2010) also argued three characteristics of information security management system (ISMS):

1. **Management-oriented:** ISMS emphasis on managerial issues, such as the development of security policy, risk management, business continuity plan, and compliance (ISO, 2005b).

2. **Continuous improvement:** the continuous improvement process and compliance audits of ISMS (i.e., the PDCA continuous improvement process) allow organizations to detect and correct errors.

3. **Change in the social structure of organization:** the assimilation of ISMS involves the creation of a security culture and expansion of employees' knowledge capability, thus induces changes of employees' attitudes and sense of responsibility.

From the arguments above, we regard ISMS as an administrative innovation, but organizations must faces some kind of pressures or incentives to make the adoption decision. The implementation process of ISMS is very costly, therefore for those organizations that adopt ISMS, there must be some reasons. Our goal in this research is trying to find out the drivers in an organization to adopt such an administrative innovation.

3.2 Diffusion of Innovations Theory

The slow and often unexpectedly painful adoption of information technology (IT) innovations (Attewell, 1992; Lyytinen, 1991) has lead scholars and practioners to seek to understand, manage and predict its diffusion.

One popular account to explain and predict innovation adoption intentions is diffusion of innovation theory (DOI) as propagated by Rogers (2003). The DOI tradition draws upon rational theories of organizational life adopted from economics, sociology and communication theory. It develops predictive accounts of the diffusion phenomenon that supposedly helps technology implementers advance the diffusion of selected technologies. DOI theory has gained wide popularity in the IT field, and Prescott and Conger (1995) found over 70 IT articles published in IT outlets between 1984 and 1994 that relied on DOI theory. The suitability of diffusion of innovation theory in explaining the adoption intention were studied in previous studies, for example, Chin and Gopal (1995) examined the relative importance of the belief constructs (relative advantage, ease of use, compatibility, and enjoyment) in predicting GSS adoption intention. Tan and Teo (2000) proposed the framework that postulated a person's intention to adopt Internet banking is determined by three factors including their attitudes (perception towards Internet banking measured by the factors of diffusion of innovations theory). Teo et al. (1995) studied six factors potentially affecting adoption intention of organizations for financial EDI and assessed the ability of innovation diffusion theory to predict the adoption intention. Plouffe et al. (2001) found the Perceived Characteristics of Innovating (PCI) set of antecedents explains substantially variance of adoption intentions.

Taylor and Todd (1995) suggested that the different dimensions of attitudinal belief toward an innovation could be measured using the five perceived attributes of an innovation: (1) relative advantage, (2) compatibility, (3) complexity, (4) trialability, and (5) observability. The four factors are generally positively correlated with the adoption intention while the last factor, complexity, is generally negatively correlated. These attributes, originally proposed in the diffusion of innovations theory (Rogers, 2003)

1. **Relative Advantage**. Relative advantages defined by Rogers (2003) as ” the degree to which an innovation is perceived as being better than the idea it supersedes”. Tornatzky and Klein (1982) found relative advantage to be an important factor in determining adoption of new innovations. Relative advantage may be expressed in economic profitability, but it also can be measured in other ways, such as measured in terms of social benefits, time saved, or hazards removed (Tornatzky & Klein, 1982). In general, perceived relative advantage of an innovation is positively related to its rate of adoption (Rogers 1983).

2. **Compatibility**. Compatibility is the degree to which an innovation is perceived as consistent with the existing values, needs, and past experiences of the potential adopter. If the IS are compatible with existing work practices, the organizations will be more likely to adopt them. In Tornatzky and Klein’s meta-analysis of innovation adoption, they found that an innovation is more likely to be adopted when it is compatible with individuals’ job responsibilities and value system (Tornatzky & Klein, 1982).

3. **Complexity**. Complexity refers to the degree to which an innovation is perceived as difficult to use. The perceived complexity of an innovation is expected to influence the decision to adopt it negatively. Past research has indicated that an innovation with substantial complexity requires more

technical skills and needs greater implementation and operational efforts to increase its chances of adoption (Cooper & Zmud, 1990; Dickerson & Gentry, 1983).

4. **Trialability**. Rogers (2003) argued that potential adopters who are allowed to experiment with an innovation will feel more comfortable with the innovation and are more likely to adopt it. Thus, if customers are given the opportunity to try the innovation, certain fears of the unknown may be minimized. This is especially true when customers find that mistakes could be rectified, thus providing a predictable situation.

5. **Observability**. If the benefits of an innovation are visible to intended adopters, it will be adopted more easily. Initiatives to make more visible the benefits of an innovation (e.g., through demonstrations) increase the likelihood of their assimilation (Meyer & Goes, 1988)

The trialability and observability were discarded from our considerations. Since the ISO 27001 is impossible to be “tried” and then decide whether the organization should adopt or not. The changes that bring by adopting ISO 27001 cannot be reversed, so it has no trialability characteristic. Observing the benefits of ISO 27001 is hardly possible in Taiwan, because the organizations are not willing to reveal the security incidents and loss they confronted, even though the ISO 27001 can bring great benefits for the organizations, it could hardly be seen by outsider. Moreover, the administrative innovation is also less observable than technological innovation, and there are no absolute objective standards by which to evaluate an administrative innovation’s efficacy (Frost & Egri, 1991). Hence, we take out these two factors from our model because the ISO 27001 is lack of the trialability and observability characteristics.

3.3 Institutional Theory

Drawing out from the diffusion of innovation perspective, another theory that is also widely used to explain and predict innovation adoption intentions is institutional theory. Institutional theory is a theory studying the influences of institutional pressures (e.g. economics, social, and political pressures) that affect organizations (Scott, 2001). Institutional theory argues that organizations face institutional pressures to conform to the shared notions of appropriate forms and behaviors, organizations therefore have to make decisions that comply with external or internal expectations. Violating those notions may call into question the organization's legitimacy and thus affect its ability to secure resources and social supports (Teo, et al., 2003).

DiMaggio and Powell (1983), in their eminent paper, pointed out what make organizations so similar are the institutional isomorphic processes. While organizations face institutional pressures and conform to those standards or regulations, their organizational structure, culture, and output become toward homogenization. The process of homogenization called *isomorphism*, which is a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions (Hawley, 1986). DiMaggio and Powell (1983) described three basic types of institutional isomorphism, *coercive, mimetic*, and *normative* isomorphism that lead to this outcome.

1. **Coercive**: coercive isomorphism results when organizations acquire to the formal and external pressures exerted upon them by other organizations upon which they are dependent, and the cultural expectations in the society within which the organizations function. It also arises from government regulations

and policies (DiMaggio & Powell, 1983; Liang, et al., 2007; Teo, et al., 2003).

2. **Mimetic**: mimetic isomorphism occurs as organizations respond to uncertainty by mimicking actions of other organizations. Uncertainty is a powerful force that cause imitation, for instance, when technologies are poorly understand, organizations may model themselves after other organizations perceived to be legitimate or successful (DiMaggio & Powell, 1983).

3. **Normative**: Normative isomorphism stems primarily from professionalization, which is "*the collective struggle of members of an occupation to define the conditions and methods of their work, to control the production of the future member professionals, and to establish a cognitive base and legitimization for their occupational autonomy"* (DiMaggio & Powell, 1983). It occurs when managers and professionals share the norms among members (Teo, et al., 2003).

Institutional theory and innovation adoption

Institutional theory is one of the remarkable theories while researching the influence of external social, technical, and political environments on organizational behavior, e.g. adoption and assimilation of innovations (Liang, et al., 2007). "*The institutional approach to the study of organizations has led to significant insights regarding the importance of institutional environments to organizational structure and actions"* (Teo, et al., 2003). There are many studies have used this approach to study the influences of institutional isomorphism on adoption or assimilation of innovation (Chatterjee, et al., 2002; Hsu, et al., 2010; Iacovou, et al., 1995; Liang, et al., 2007; Teo, et al., 2003). Bjorck (2004) also argued the suitability of institutional theory for the study of IS/IT security in organizations, but there is little research using this approach. While the emerging of needs of information security standards, the reasons why organizations decided to adopt ISO 27001 are no longer simply for “competitive advantage”, “compliance”, or “reputation”. As organizations compete for resources, customers, or others, the organizations decided to adopt ISO 27001 possibly for legitimacy, social fitness, or requirements of other organizations. In such institutional environments circumstance, identifying what institutional forces affect organizations’ behavior is especially important for modern IT/IS security research and for a manager who wants to adopt ISO 27001.

3.4 Research Model

In our research model, we introduced the main forces in DOI theory and institutional theory as well as several control variables to develop the model.

3.4.1 Relative Advantage

Relative advantage is the degree to which an innovation is perceived as better than its precursor (Rogers, 2003). It has been largely treated as identical to perceived usefulness (Adams, et al., 1992; Plouffe, et al., 2001). That is, the positive perceptions of the benefits of IS should provide an incentive for the organizations to adopt the innovation. One of the most important benefits of implementing ISO 27001 is the improvement of control and process management. It can help the organizations move from a technical focus to a more business-led focus of information security and define the responsibilities and roles of related personnel clearer. Hence, our first hypothesis is,

H_1: The greater the perceived relative advantage of ISO27001 the more likely they will be adopted.

3.4.2 Compatibility

Compatibility: organizations are more likely to adopt a technology if they perceive that it is consistent with their culture, values, preferred work practices, and existing IS infrastructure. Because the adoption of ISO 27001 requires adopting firms to modify existing business practices and processes, the compatibility of an organization can impact the adoption decision. In our study, we focus on whether the organization's process compatible with ISO 27001. There is a positive relationship between organizational compatibility and ISO 27001 adoption intention. Hence we hypothesize:

H_2: The greater the perceived compatibility of ISO 27001 with current business processes, the more likely they will be adopted.

3.4.3 Complexity

Complexity is the degree of difficulty in understanding an innovation. The introduction of a new innovation can be intimidating for organizational employees. The ISO 27001 influences the business processes and requires all the employees to comply with the requirements of ISO 27001, hence the intricacies of ISO 27001 for the employees and manages could be a hindrance leading to the decision of adopting ISO 27001. Therefore, our hypothesis is that:

H_3: The greater the perceived complexity of ISO 27001 the less likely they will be adopted.

3.4.4 Coercive Pressures

Coercive isomorphism results from both formal and informal pressures exerted on organizations by other organizations (DiMaggio & Powell, 1983). The coercive pressures such as legal requirement, customers' demand, and competition necessity affect many aspects of an organization's behavior and structure. Hence, we postulate that:

H_4: Greater coercive pressures results in a greater adoption intention of ISO27001.

Legal requirements, for financial institutions and corporations, they have to comply with regulation and legislation such as Sarbanes–Oxley and Basel II. If they did not comply with those regulations in certain period of time, they have to pay a large amount of fine. As mentioned earlier, adopting ISO 27001 helps them to meet the requirements of various regulations (ISO, 2005b; von Solms, 1999). Compliance with certification in ISO 27001 will give an organization strong IT-related controls that could satisfy the requirements of many regulatory standards (Brenner, 2007). Hence, we have the first corollary to H_4:

H_{4a}: Greater perceived pressures of legal requirements results in a greater adoption intention of ISO 27001.

Customer requirements, for those organizations which are not directly affected by the regulations sometimes also needed to adopt certain controls and certifications, because they sometimes are forced by their customers. The customers which are coerced by the regulations or simply afraid of their confidential information may be compromised often makes requisition to its suppliers to demonstrate superior information security performance (Ezingeard & Birchall, 2005). Therefore, the second corollary to H_4 is:

H_{4b}: Greater perceived pressures of customer requirements results in a greater adoption intention of ISO27001.

3.4.5 Mimetic Pressures

Mimetic pressures cause one organization to behave more like other organizations (especially those successful organizations) over time. In the speedy changing environment today, it’s not rare that organizations are uncertain about whether they should adopt one new standard or not, especially while there are usually not much evaluations or information about a new standard. That is, the mimicry fundamentally occurs from the uncertainty about the environments. For now, we have the fifth hypothesis that:

> **H_5: Greater mimetic pressures results in a greater adoption intention of ISO27001.**

Haunschild & Miner (1997) distinguished three types of selective inter-organizational imitation (i.e. frequency-based imitation, trait-based imitation, and outcome-based imitation), and these imitation modes are occur independently. The outcome-based imitation was discarded because similar to observability, the outcomes of adopting ISO 27001 can hardly be seen. Therefore we only take the frequency- and trait-based imitation into our model.

Frequency-based imitation; organizations tend to imitate the actions that have been undertaken by large numbers of other organizations, because the legitimacy of taking such actions are enhanced. The imitation effect occurs because the desire for legitimacy leads firm to adopt legitimate practices (Haunschild & Miner, 1997; Meyer & Rowan, 1977). This effect also could occur unconsciously, that is, when a practice is prevalent among large numbers of organizations, it becomes increasingly taken-for-granted so that some organizations may adopt such practice without deliberations (Haunschild & Miner, 1997; March, 1981; Zucker, 1977). Hence, the large number of other organizations enacting a practice enhances legitimacy and endows a practice with a taken-for-granted status. In the context of information security, the more widespread of a standard may cause a higher probability of an organization deciding to adopt the standard. Hence, the corollary to H_5 is:

H_{5a}: The greater extent of adoption of ISO27001 among its competitors will results in a greater adoption intention of ISO27001.

Trait-based imitation; compare to frequency-based imitation, trait-based imitation is a more selective form of mimetic process, in which a organization imitate practices that have been used by other organizations that with certain features such as large size, success, and high status. Trait-based imitation may derive from the beliefs that imitating the prominent organizations is a reasonable strategy to cope with uncertainty and that it may lead to gains in legitimacy (Jeyaraj, et al., 2009). The second corollary to H_5 is:

H_{5b}: The greater number of successful organizations that adopted ISO 27001 results in a greater adoption intention of ISO27001.

3.4.6 Normative Pressures

Frequent communication between two or more individuals (often professionals) results in that they are more likely to think and behave similar to each other in the same social network. This result may lead to the third pressure (i.e. normative pressures) that causes the isomorphism. We identify two important sources that lead to this result: *participations in trade and professional associations* and *managers' background*. The sixth postulation is:

H_6: Greater normative pressures results in a greater adoption intention of ISO27001.

Participations in trade and professional associations; normative rules about organizational behavior are defined and promulgated through active participation in a wide array of events such as conferences, workshops, and educational programs organized by trade and professional associations. Individuals participating in these events or subscribing to the professional publications of these associations would learn the acceptable norms of practices and affect the behavior of their organization accordingly. In the context of information security, we focus on the organizations' participations of security relating associations and publications. Hence the corollary to H_6 is:

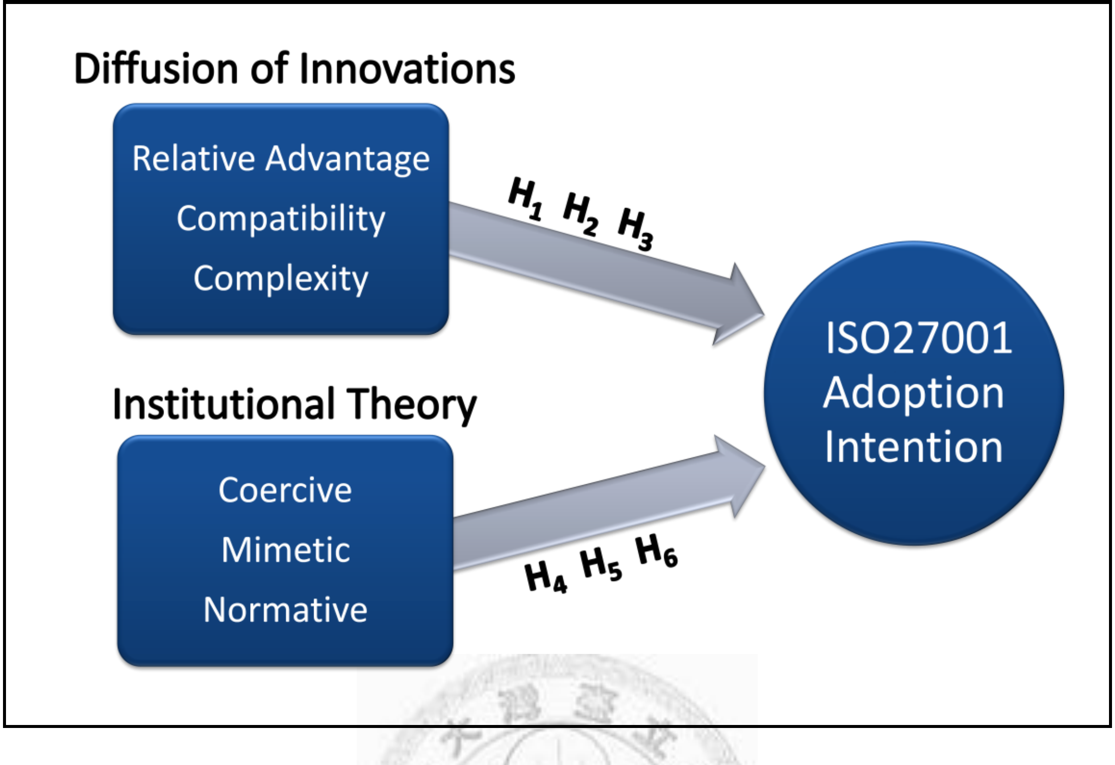
> **H_{6a}: The more active participations of an organization in professional and trade associations results in a greater adoption intention of ISO27001.**

Managers' background (e.g. CIO, CSO, CISO, or other managers), for those managers that have the same education background (for instance, they may have the same academic degree, graduated from the same school, or got the similar certifications) often make similar decisions. They possibly read the same materials, have the similar knowledge of current circumstance, and take the same point of view about the problems. Moreover, the wider extent of IT Security related background managers will result in higher normative activities. More specifically, the numbers could be another indicator of normative pressures that make the organizations to make similar decisions, i.e., to adopt ISO 27001. Therefore we got the second corollary to H_6:

> **H_{6b}: Greater extent of managers with IT Security background results in a greater adoption intention of ISO27001.**

The full research model that integrating the factors form diffusion of innovation and institutional theories is shown is figure 3-1 below. After developing our research framework, we want to test our model by collecting and analyzing the empirical data. In next chapter, we will discuss the designs and methodologies in detail.

Figure 3-1: The Research Model



Chapter 4 Research Design

In this chapter, we will discuss how we develop the measures of independent and dependent variables that we identified in previous chapter and several control variables that might influence the adoption decision will also be provided. The sampling sources, procedures and the research methodologies that used to test our model and hypotheses will also be introduced in this chapter. The questionnaire used in this study is developed mainly based on the literature of information systems and information security.

4.1 Measures

We selected and developed the measurements of constructs from the literature, and the detailed items sources are provided in the following subsections. We verified the items on the questionnaire and the operational concepts from the test to prevent overlap and these items are reviewed by several experts who are currently working in the field of information security and providing the consulting services, and that ensures the face and contents validity of survey instruments. Empirical literature on innovations diffusion and institutional theories are examined for validated measures of the constructs (i.e. relative advantages, compatibility, complexity, mimetic pressures, coercive pressures, and normative pressures).

4.1.1 Independent Variables

All the measurement scales used to operationalize constructs of independent variables in this study are grounded in the previous research and theory and all indicators representing the research constructs of independent variables were measured using a seven-point Likert-type scale ranging from strongly disagree (1) to strongly agree (7).

Diffusion of innovations theory

Relative advantages; three items accessing the relative advantage were adapted from Lai (2008). Since the ISO 27001 is an administrative innovation, one of the most important advantages is that ISO 27001 helps the organization improve their management. Therefore, the items ask respondents to access whether they think the adoption of ISO 27001 could improve the managing of information, reducing the impact of information incidents, and clarifying the roles and responsibility of employees. This construct was operatonalized as formative concept from the three items, and using 7-point Likert scale.

Compatibility was measured as a formative construct. The change of business process is inevitable in order to adopt and implement ISO 27001, therefore the more compatible the current business of the organization with ISO 27001, the more possible the organization will adopt. There are three items in this construct and the items were adapted from Lai et al. (2008) and Teo et al. (2007), and the items include the whether the current process compatible with ISO 27001, whether integrate ISO 27001 with business process is easy, and whether the original process contains security considerations. The items of measuring compatibility are also using 7-point Likert scale.

Complexity; This construct was also measured as formative, and there are three indicators were used to measure complexity, tapping into aspects of difficulty of understanding the contents of ISO 27001, the effort needed during the implementation of ISO 27001, and the overall complexity of ISO 27001 implementation. The items were adapted from Teo et al. (2007) and Ramamurthy et al. (2008). The items of complexity are also measured in 7-point Likert scale.

Institutional theory

Coercive pressures; we operationalized coercive pressures as a formative construct formed from two subconstructs (i.e. legal requirements and customers requirements). The question items of coercive pressures constructs was developed from literatures: legal requirements items were adapted from Lai et al (2008) and Chen et al (2009) and items of customers' requirements were adapted from Khalifa and Davison (2006). The subconstructs were measured by asking respondent to indicate at what extent their organization's perceived the pressure from regulations and customers.

Mimetic pressures construct was also operationalized as a formative construct formed from two subconstructs: frequency-based imitations (i.e. the extent of adoption by competitors) and trait-based imitations (the characteristics of the adopters). The theoretical rationale is that the imitation of extent of adoption by competitors is not necessarily correlated with the imitations of the successful/leading organizations (Haunschild & Miner, 1997). A seven-point scale was used to gauge the construct items which developed from the past researches that frequency-based imitations items were adapted from Son and Benbasat (2007) and trait-based imitations items were adapted from Lai et al (2008)

Normative pressures could arise from members of dyadic relational channels and multilateral organizations such as professional, trade, and industry organizations. Hence, as argued for the cases of mimetic and coercive constructs, we operationalized the normative pressures construct as a formative construct formed by two subconstructs: the participation in professional, trade, and business bodies that promote and disseminate information on ISO 27001 adoption and the extent of the managers' background (information security related education and/or certifications). Normative influence from institutional members was gauged by asking at what extent the respondents were members of any professional, trade, or business associations that endorse ISO 27001 and the extent of managers who had information security related education/certifications, because organizations are apt to act collectively when they are members of these associations and have the same background.

The constructs of institutional pressures were measured and coded in the same way as innovations diffusion variables (i.e. 7-point Likert scale).

4.1.2 Dependent Variable

Adoption intention; for the adoption intention, first we asked the respondents to indicate what their organizations' situation about their information security managements; whether they were already adopted information security management standard (and when they adopted the standard), they were contemplating the adoption, or they had no such plan yet. If they were assessing the adoption, next we ask the respondents indicate their intention about ISO 27001 adoption by asking whether (1) they were contemplating to adopt ISO 27001, (2) they were likely to adopt ISO 27001 in the near future, (3) they were discussing and considering to adopt ISO 27001. The adoption intention was measured as reflective construct and all the question items were adapted from previous research, i.e. Teo et al.(2003). The adoption intention items in the questionnaire were anchored on appropriately labeled 7-point scales. However, if the organization had already adopted ISO 27001, we coded the intention as 7 (strongly agree) throughout the three intention items.

The summary of each constructs and related items sources are shown in table 4-1 below.

Table 4-1: Summary of Research Constructs and Sources

Constructs	Items[5]	Short Descriptions	Sources
Relative Advantages	RA_1	Improving the manages and controls of information	(Lai, et al., 2008)
	RA_2	Reducing the impact of information security incidents	
	RA_3	Clarifying the roles and responsibilities of employees	
Compatibility	CMPT_1	Easy to integrate the current process with ISO 27001	(Teo, et al., 2007; Zhu, et al., 2006)
	CMPT_2*	Modifying business process to comply with ISO 27001	
	CMPT_3	Original process contained security considerations	
Complexity	CMPX_1*	Understand ISO 27001 is easy for our employees	(Ramamurthy, et al., 2008; Teo, et al., 2007)
	CMPX_2	Training efforts during the ISO 27001 implementation	
	CMPX_3	The implementation process of ISO 27001 is complex	
Coercive Pressures – Legal Requirements	CPL_1	Law/competent authority require us to adopt ISO 27001	(Chen, et al., 2009; Lai, et al., 2008) (Khalifa & Davison, 2006)
	CPL_2	Current/future regulation drive us to adopt ISO 27001	
	CPL_3	Comply with law/regulation if adopting ISO 27001	
Coercive Pressures – Customers' requirements	CPC_1	Our clients think we should adopt ISO 27001	
	CPC_2	Adopt ISO 27001 in order to deal with our clients	
	CPC_3	Our main clients urge us to adopt ISO 27001	
Mimetic Pressures – Frequency-based Mimicry	MPF_1	Many companies already adopted ISO 27001	(Son & Benbasat, 2007)
	MPF_2	Many companies will adopt ISO 27001 recently	
	MPF_3	Many our competitors already adopted ISO 27001	
Mimetic Pressures – Trait-based Mimicry	MPT_1	The adopted ISO 27001 companies usually are large	(Lai, et al., 2008)
	MPT_2	The adopted ISO 27001 are leading companies	
	MPT_3	The adopted ISO 27001 are successful companies	
Normative Pressures – Participation in Associations	NPP_1	Many pressures force us to participate in associations	(Son & Benbasat, 2007)
	NPP_2	We actively participate in the associations	
	NPP_3	We frequently pay attention to the associations	
Normative Pressures – Managers' Background	NPM_1*	Few managers with security background in our industry	
	NPM_2	Many security background managers in our IT dept.	
	NPM_3	Many security background managers in others' IT dept.	
Adoption Intention	AI_1	We are anticipating adopting ISO 27001	(Teo, et al., 2003; Teo, et al., 2007)
	AI_2	We are likely to adopt ISO 27001 in the future	
	AI_3	We are contemplating to adopt ISO 27001	

[5] Items with star sign (*) indicate the item was reverse coded.

4.2 Control Variables

Prior research on innovation adoption studies and the feedback from our reviewer suggest that some additional factors should be included because of their potential influence on organizational adoption intention. Hence we included some control variables such as industry types, organization size, IT department size, IT budget, and information security budget.

Industry type could be one important consideration since the different industry may receive different level of pressures. For example, the government departments, universities, colleges, schools (including high schools and elementary schools), and financial/banking institutions are receiving more coercive pressures because of the laws in Taiwan.

Organization size has been found to have a positive influence on adoption behavior (Rogers, 2003). Large organizations possess the resources and the necessary skills to assimilate that innovation effectively and also process the economies of scale in transactions to leverage their investment in the innovation, so they are more likely to adopt an innovation than small organizations (Rogers, 2003; Teo, et al., 2003). The influence of organization size was considered in many innovation studies as a surrogate measure for total resources and slack resources. We used the capital and number of organization employees as indicators of organizations size.

IT department size represents the technical resources an organization possesses to effectively assimilate an innovation, e.g. Damanpour (1991). Technical resources have been found to be extremely important in adoption of technological innovations, e.g. Zmud (1984) because the larger the department size, the broader the technological knowledge base of the organization for introducing and deploying innovations (e.g.

ISMS). The number of IT department employees was used to measure the IT department size.

IT budget and information security budget can be the indicator of how important an organization see their IT and information security. If the budget is relative high among with their competitors that have similar organization size, it represents that the organization regards IT and Information security are important (relative to its competitors). The organizations that emphasize on IT will more likely adopt IT security-related standards than those do not regard IT as an important element for them, thus the budget of IT/IS is an indicator of their attitude toward IT/IS, and the attitude will influence the intention of adopting ISO 27001.

In addition to the independent, dependent, and control variables items, some other question items including "current state of information security management systems", "the extent of the information security management systems", and "number of information security management systems team" were also surveyed. The detail survey items were shown in appendix B.

4.3 Data Collection and Sample

In order to make the sample to be diversity, our questionnaires were distributed to several places and means, including the online forums, information security related conferences, and the usual meeting of Information Systems Audit and Control Association (ISACA) in Taiwan.

Online forums, including the forum of Information & Communication Security Technology Center (ICST) and the largest Bulletin Board System (BBS) in Taiwan, the former is a well-known online forum discussing information security related topics and the other is a large BBS site discussing different topics in separated public message boards in the BBS site. In order to collect the opinions from various industries, we distributed questionnaire to the boards such as Tech-Job, Soft-Job, Finance, etc.

Information security conferences; we also contact several information security related conferences, but unfortunately only one conference allowed us to conduct the survey. The conference was about the law of personal data protection and enterprise security and it was hold by Chalet Tech. and TrustView Inc.

Information Systems Audit and Control Association (ISACA), which is a global organization for information governance, control, security and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide, and research pinpoints professional issues challenging its constituents. The members of ISACA live and work in more than 160 countries and cover a variety of professional IT-related positions including IS auditor, consultant, educator, IS security professional, regulator, chief information officer, internal auditor, etc. Some are new to the field, others are at middle management levels and still others are in the most senior ranks. They work in nearly all industry categories, including financial and banking, public accounting, government and the public sector, utilities and manufacturing. This diversity enables members to learn from each other, and exchange widely divergent viewpoints on a variety of professional topics. It has long been considered one of ISACA’s strengths. And because of the strengths of ISACA, we believe the distributions of questionnaire could reach more easily and directly to IT-related and information security related employee or mangers in diverse industries.

We expect the various sources of questionnaires allow our results to apply to different industries in Taiwan, and hence the model could be a generalized model rather than a model that specific in one industry.

4.4 Analysis Method

As a primary data analysis method, Structural Equation Modeling (SEM) was used to find the relationship among latent constructs described in our theoretical framework. Structural equation modeling is not a single statistical technique, but rather a family of statistical tools that are similar to other statistical tests like regression, factor analysis, and path diagrams. Structural equation modeling can be used in exploratory factor analysis, confirmatory factor analysis, path analysis, models with latent factors, and linear growth curve analysis for longitudinal data (Kline, 2005). While SEM is similar to regression, it has many advantages over regression. First, violations of assumptions and issues with one's data do not restrict one's interpretation of results in the same manner as it does in regression due to more complex estimation techniques. Also, the ability to use confirmatory factor analysis in SEM allows the researcher to build models including latent factors designed to measure an unobserved concept.

The SEM technique is a confirmatory technique based on previous theory in contrast to exploratory factory analysis. Researchers must think about data screening before conducting an analysis. All data were screened by the Statistical Package for the Social Sciences (SPSS) 17.0 version. The program Analysis of Moment Structures (AMOS) 17.0 computer software was used to estimate the framework (model) for our research hypotheses.

Before analysis of data, researchers must think about the practical issues of SEM: sample size, missing data, multivariate normality, and outliers. When researchers use SEM analysis, researchers frequently pass over the problem of sample size. Hair et al.(2006) suggested that researchers must decide the sample size by considering the model complexity and model characteristics, because covariance in SEM is very sensitive to sample size. Hair et al. (2006) said that "if a SEM model contains five or fewer constructs, or any communality is modest, or the model contains constructs with fewer than three items, then the required sample size is more on the order of 200". If researchers find missing values, the input of missing values is effective, especially when deleting missing values is a serious problem. If the number missing data is high and the data are missing at random, the Expectation Maximization (EM) method of data imputation must be used. If outliers distort information, outliers must be removed.

The most important assumption of SEM is multivariate normality. If measured variables are violated in univariate and multivariate normality, SEM results in incorrect outcomes. Researchers should check the normality through scrutinizing the skewness and kurtosis of the measured variables. All measured variables must be screened for outliers. If researchers find significant skewness or kurtosis, the transformations or deleting of outliers should be considered. If the results found by analysis of the transformed data is same as the results using raw data, the original data are used. After transformation, if the data do not show normality, an estimation method of non-normality should be selected.

Structural equation modeling (SEM) is a multivariate technique to simultaneously analyze the relationships among the measured variables and latent constructs. Maximum Likelihood Estimation (MLE), which is widely used as an estimate technique, was applied in this SEM analysis. Hair et al. (2006) said that "MLE is the most efficient and unbiased estimation method, when the assumption of multivariate normality is met" (p. 743). I followed three procedures to apply SEM. First of all, we examine the goodness-of-fit of each indicator. Second, in a simultaneous analysis, we examined all of the relationships in the structural model. A more specific analysis to find relationships between constructs was made last.

Goodness-of-fit (GOF) indices were applied to assess model validity. GOF shows the similarity of the observed and estimated covariance matrices. If researchers find similarity in covariance, we can say that the measurement model represents reality well. Kline (2005) explained that most clear evidence that a model fit well is a Chi-square test ($\chi2$ statistic) with $p >.05$. A p-value greater than .05 indicates no statistically significant difference between the covariance. Multiple fit indices are used to accept a SEM model, because the chi-square to test overall model fit is sensitive to sample size and is influenced by the difference in covariance matrices (Hair, et al., 2006; Kline, 2005). Three kinds of goodness-of-fit are commonly used in SEM studies: absolute fit indices (i.e., chi-square statistic, goodness-of-fit index, root means square residual, standardized root mean residual, root mean square error of approximation, the expected cross-validation index, the actual cross-validation index), incremental fit indices (or called relative fit index, such as normed fit index, comparative fit index, Tucker Lewis index, relative noncentrality index), and parsimony fit indices (parsimony goodness-of-fit index, parsimony normed fit index). Most researchers agree that the basic chi-square test with degrees of freedom, and one or more absolute fit and one or more incremental fit indices should be reported. In this study, the Chi-square test with degrees of freedom, the root mean square error of approximation (RMSEA), the comparative fit index (CFI), normed fit index (NFI) and parsimony adjustments to the CFI (PCFI) and NFI (PNFI) were selected to assess the overall fit of the model. The meaning of these indices will be discussed in chapter 5.

Chapter 5 Results and Discussions

This chapter provides an analysis of data in light of the research questions. First, we examined the profile of the sample. Second, we scrutinized the reliability, validity, and descriptive statistics (means, standard deviations, and) of the variables. Third, prior to SEM analysis, we check the normality of data, ensuring the data met the assumption of normality. Then we executed the SEM techniques and examined the goodness-of-fit indices to evaluate our model, and the hypotheses testing and discussion were made last in this chapter.

5.1 Sample Characteristics

As discussed in the previous chapter, data were collected from several sources by means of internet-based and paper-based survey. We gathered a total of 56 respondents, 35 are internet-based and 21 are paper-based. However, in the internet-based survey, 2 of the questionnaire were regarded as invalid. Because one responded the straight 1 and another responded straight 7 through all items, ignoring the reverse coded items, hence we considered the two responses were invalid and deleted before further analysis. In the paper-based survey, there were 2 invalid responses since they did not response the dependent variable items (i.e. none of the items of adoption intention were answered), therefore we could not use such data to gain any information of the relation between independent and dependent variables. Also, we deleted the 2 invalid responses before conducting further analysis.

The profiles of the respondent organizations are shown in table 5-1. For the variables, the numbers are well distributed in each category, showing the classifications are well discriminate between different organizations. One affair should be addressed is that the budgets of IT and security contained many missing values (31 out of 52 are missing values), and we thereby cannot use the two variables in SEM analysis because of the high proportion of missing values. Although the two budget variables cannot be used in analysis procedure, we found the budgets are highly correlated with number of IT employees (also significant), hence we believe the results produced by SEM should be robust and reliable even without the two variables.

5.2 Descriptive Statistics and Reliability and Validity Assessment

The descriptive statistics (mean and standard deviation) of dependent, independent, and control variables were shown in table 5-2. The reliability and validity information (factor loading and average variance extracted) were also shown in the table. Other descriptive statistics such as skewness and kurtosis of each variable will be reported later in table 5-4.

The instruments were tested for validity and reliability properties, while the validity is the extent to which a test actually measures what it purports to measure and reliability is the extent to which a variable or set of variables is consistent in what it is intended to measure (Churchill, 1979; Hair, et al., 1995). Before performing the structural equation modeling, the examinations of constructs reliability and validity are necessary. In the following subsections, we examine the reliability and construct validity.

Table 5-1: Profiles of Respondent Organizations

Industry Type

Industry	Frequency	Percentage
Governmental departments	**3**	**5.8**
Universities & schools	**4**	**7.7**
Tech & manufacturing	**28**	**53.8**
Service industry	**6**	**11.5**
Medical agencies	**1**	**1.9**
Finance	**5**	**9.6**
Other	**5**	**9.6**

Capital (million)

Range	Frequency	Percentage
Not applicable (ex. school)	**8**	**15.4**
Less than 10	**2**	**3.8**
10 – 30	**3**	**5.8**
30 – 50	**4**	**7.7**
50 – 100	**3**	**5.8**
100 – 500	**4**	**7.7**
500 – 2000	**7**	**13.5**
2000 – 5000	**3**	**5.8**
5000 – 10000	**2**	**3.8**
More than 10000	**16**	**30.8**

IT Department Employee

Range	Frequency	Percentage
Less than 15	**20**	**38.5**
16 – 30	**7**	**13.5**
31 – 60	**4**	**7.7**
61 – 100	**5**	**9.6**
101 – 200	**1**	**1.9**
201 – 300	**5**	**9.6**
301 – 500	**6**	**11.5**
More than 500	**4**	**7.7**

Respondents’ position

Position	Frequency	Percentage
Chief Information Officer	**5**	**9.6**
Chief Information Security Officer	**0**	**0**
CIO & CISO	**3**	**5.8**
IT department employee	**21**	**40.4**
IT security employee	**5**	**9.6**
Other	**18**	**34.6**

Employee

Range	Frequency	Percentage
Less than 100	**12**	**23.1**
101 – 200	**1**	**1.9**
201 – 500	**6**	**11.5**
501 – 1000	**7**	**13.5**
1001 – 2000	**6**	**11.5**
2001 – 5000	**9**	**17.3**
5001 – 10000	**4**	**7.7**
More than 10000	**7**	**13.5**

States of organizations’ ISMS

State	Frequency	Percentage
No any ISMS planning and not assess any ISMS yet	**19**	**36.5**
Assessing the ISMS adoption, but haven’t decided which ISMS will be adopted	**9**	**17.3**
Already decide other ISMS rather than ISO 27001	**2**	**3.8**
Already adopted ISO 27001 and are implementing it	**2**	**3.8**
Already get the ISO 27001 certificate	**19**	**36.5**
Already get the ISO 27001 certificate, but wont maintain it anymore	**1**	**1.9**

Table 5-2: Descriptive Statistics of Variables and Constructs

Construct	Reliability	AVE	Variable	Mean	Std. Deviation	Loading[6]
Control Variables	N/A	N/A	IT_employee	3.35	2.558	N/A
			Employee	4.38	2.427	N/A
			Capital	6.33	3.353	N/A
Relative Advantage	0.967	0.938	RA_1	4.85	1.673	0.966
			RA_2	4.94	1.614	0.981
			RA_3	5.12	1.665	0.910
Compatibility	0.828	0.742	CMPT_1	3.71	1.576	1.040
			CMPT_2	4.06	1.673	0.683
			CMPT_3	4.63	1.387	0.613
Complexity	0.817	0.353	CMPX_1	5.02	1.057	0.463
			CMPX_2	5.63	1.284	0.308
			CMPX_3	5.63	1.121	0.335
Coercive Pressures Legal requirements	0.888	0.823	CPL_1	3.60	1.943	0.721
			CPL_2	4.48	1.777	1.013
			CPL_3	4.83	1.779	0.866
Coercive Pressures Customers' requirements	0.919	0.857	CPC_1	4.06	1.731	0.753
			CPC_2	3.88	1.947	0.947
			CPC_3	3.77	1.733	0.979
Mimetic Pressures Frequency-based mimicry	0.927	0.874	MPF_1	4.12	1.665	0.897
			MPF_2	4.13	1.657	0.921
			MPF_3	3.94	1.776	0.884
Mimetic Pressures Trait-based mimicry	0.957	0.923	MPT_1	5.12	1.491	0.888
			MPT_2	4.98	1.686	1.002
			MPT_3	4.83	1.654	0.932
Normative Pressures Participation in associations	0.901	0.836	NPP_1	4.29	1.673	0.741
			NPP_2	4.13	1.560	1.044
			NPP_3	4.21	1.613	0.832
Normative Pressures Managers' background	0.898	0.832	NPM_1	3.79	1.564	0.757
			NPM_2	4.15	1.613	1.041
			NPM_3	3.98	1.336	0.795
Adoption Intention	0.977	0.958	AI_1	5.04	2.009	0.953
			AI_2	5.48	1.809	0.943
			AI_3	5.33	1.865	0.951

[6] They are standardized loadings reported by AMOS, all loadings are significant at p-value = 0.05, except CMPX_2, which the p-value is 0.053 (that is very close to the significant level).

5.2.1 Reliability

In order to increase reliability, the multiple items were used to operationalize for each construct. The reliabilities of the constructs were assessed using Cronbach's alpha (Cronbach, 1951; Nunnally & Bernstein, 1978). While internal consistencies using Cronbach's alpha of 0.8 or above are considered adequate, an alpha of 0.7 and above is considered acceptable (Fornell & Larcker, 1981; Nunnally, et al., 1994). The results of descriptive statistics of study constructs and control variables, including constructs' reliabilities, were shown in table 5-2. In our study, all of the reliabilities of constructs are higher than 0.8 and thus the constructs are adequate and reliable.

5.2.2 Validity

Construct validity was evaluated by examining the factor loading within the constructs as well as the correlation and average variance extracted (AVE) between the constructs. The construct validity is usually achieved by convergent and discriminant validity (Anderson & Gerbing, 1988). The convergent validity assesses the extent to which different indicators for the measure refer to the same construct (Hair, et al., 1995; Nunnally, et al., 1994). Convergent validity is achieved when two instruments that are valid measure of the same or similar concepts should correlate rather highly with one another. On the other hand, discriminant validity of a measure assesses if the measure is adequately distinguishable from related constructs. In other words, it measures the degree to which a concept differs from other similar concepts and is indicated by the items not correlating highly with other measures from which is should theoretically differ (Anderson & Gerbing, 1988).

Convergent validity is evaluated by the average variance extracted (AVE) and factor loadings. The average variance extracted or AVE (Fornell & Larcker, 1981) reflects the amount of variance that a latent variable extracts from it indicators relative to the amount of measurement error (Chin, 1998). It is generally recommended that measures of AVE should be greater than .50, indicating that at least 50% of the variance of the indicators has been accounted for. Based on the results shown in table 5-2, complexity (i.e., CMPX) had an AVE slightly below the recommended value. Another evaluation is the factor loading, all item loading except CMPX_2 are significant at 0.05 level. However, the significant level of CMPX_2 is 0.053 that slightly higher than 0.05, hence we still retain the item. Given the measures of internal consistency, the measure was deemed acceptable.

For discriminant validity, the average variance shared between each construct and its measures should be greater than the variance shared between the construct and other constructs (i.e., the square root of AVE should be larger than the correlations between constructs or the off-diagonal elements) (Fornell & Larcker, 1981). We examined discriminant validity at the construct level. The square root of the AVE for each construct should be greater than the correlation between constructs. Table 5-3 presents each construct's inter-correlations and the square root of its AVE and the items along the diagonal in parentheses are the square roots of the AVE. In every case, the square root of the AVE is greater than the correlation coefficient involving the construct. Thus, the assessments of reliability and validity suggest that the measurement model is satisfactory.

Table 5-3: Constructs Intercorrelations and Square Root of AVE

	RA	CMPT	CMPX	CPL	CPC	MPF	MPT	NPP	NPM	AI
RA	**0.968**									
CMPT	0.643	**0.861**								
CMPX	-0.357	-0.224	**0.594**							
CPL	0.748	0.555	-0.346	**0.907**						
CPC	0.661	0.395	-0.330	0.582	**0.926**					
MPF	0.508	0.271	-0.352	0.558	0.700	**0.935**				
MPT	0.693	0.512	-0.282	0.658	0.545	0.565	**0.961**			
NPP	0.694	0.411	-0.255	0.613	0.715	0.675	0.699	**0.915**		
NPM	0.530	0.456	-0.281	0.559	0.471	0.488	0.546	0.697	**0.912**	
AI	0.720	0.455	-0.394	0.752	0.616	0.613	0.603	0.660	0.599	**0.979**

After the examinations of the constructs' reliability and validity, we ensure our data should be a reliable and valid data set, and it can be used to a further analysis to find out the relationship between the independent variables and dependent variable (i.e., whether the independents from the two theories could really influence the adoption intention). Therefore, the next step is the evaluation of normality in the data. After assuring the normality and multivariate normality, we can finally fit our data into the introduced structural models and test the hypotheses we proposed.

5.3 Normality Checking, Model Fitting and Hypotheses Testing

Since the most important assumption of SEM is multivariate normality, the violation in univariate and multivariate normality, SEM will result in incorrect outcomes. Therefore, before conducting our model fitting and hypotheses testing, we need to examine the normality of our data. The SEM is based on the analysis of covariance structures, evidence of kurtosis is always of concern and, particularly, evidence of multivariate of kurtosis, as it is known to be exceptionally detrimental in SEM analysis.

5.3.1 Normality Checking

In table 5-4, we first examine the univariate statistics from the columns of kurtosis and its critical ratio (C.R.) listed for each of the items. As shown, positive values range from 0.096 to 0.355 and negative values from -1.304 to -0.037, yielding an overall mean univariate kurtosis value of -0.538. The standardized kurtosis index in a normal distribution has a value of 3, with larger values representing positive kurtosis and lesser values representing negative kurtosis. However, the computer programs (including AMOS) rescale the value by subtracting 3 from the normal distribution kurtosis value, thereby making zero the indicator of normal distribution and its sign the indicator of positive or negative kurtosis (West, et al., 1995). Although there appears to be no clear consensus as to how large the nonzero values should be before conclusions of extreme kurtosis can be drawn (Kline, 2005), West el al. (1995) consider rescaled kurtosis value equal to or greater than 7 to be indicative of early departure from normality. Using this as a guide, a review of the kurtosis value in table 5-4 that reported from AMOS reveals that there was no item to be substantially kurtotic.

However, the presence of nonnormal observed variables preclude the possibility of a multivariate normal distribution, the converse is not necessarily true. It means that, regardless of whether the distribution of observed variables is univariate normal, the multivariate distribution still could be multivariate nonnormal (West, et al., 1995). Thus, we should examine the index of multivariate kurtosis and its critical ratio, both of which appear at the bottom of the kurtosis and critical ratio (C.R.) columns of table 5-3. Of the most important is the C.R. value, which in essence represents Mardia’s normalized estimate of multivariate kurtosis (Mardia, 1970; Mardia, 1974), although it is not explicitly labeled as such. When the same sample size is very large and multivariately normal, Mardia’s normalized estimate is distributed as a unit normal variate such that large values reflect significant positive kurtosis and large negative values reflect significant negative kurtosis. Bentler (2006) has suggested that, in practice, kurtosis values greater than 5.00 are indicative of data that are nonnormally distributed. Using this as a guideline, the statistic of 2.042 is suggestive of multivariate normality in our data.

Table 5-4: Skew, Kurtosis, and Multivariate of Variables

Constructs	Variables	skew	C.R.[7]	kurtosis	C.R.
Control Variables	IT_employee	.602	1.773	-1.199	-1.765
	Employee	-.074	-.218	-1.227	-1.806
	Capital	-.354	-1.041	-1.304	-1.919
Relative Advantage	RA_1	-.921	-2.712	.096	.141
	RA_2	-.980	-2.884	.355	.523
	RA_3	-1.009	-2.970	.310	.457
Compatibility	CMPT_1	.212	.623	-.720	-1.059
	CMPT_2	-.092	-.270	-.856	-1.260
	CMPT_3	-.527	-1.552	-.373	-.549
Complexity	CMPX_1	-.038	-.113	.220	.324
	CMPX_2	-.639	-1.882	-.741	-1.091
	CMPX_3	-.594	-1.749	-.503	-.741
Coercive Pressures Legal Requirement	CPL_1	.226	.665	-1.010	-1.487
	CPL_2	-.476	-1.403	-.491	-.722
	CPL_3	-.622	-1.831	-.391	-.576
Coercive Pressures Customers' Requirements	CPC_1	-.135	-.398	-.831	-1.223
	CPC_2	.035	.103	-1.107	-1.629
	CPC_3	.064	.187	-.789	-1.161
Mimetic Pressures Frequency-based Mimicry	MPF_1	-.210	-.619	-.569	-.838
	MPF_2	-.138	-.406	-.681	-1.002
	MPF_3	-.103	-.303	-.839	-1.235
Mimetic Pressures Trait-based Mimicry	MPT_1	-.486	-1.431	-.382	-.562
	MPT_2	-.763	-2.245	-.124	-.183
	MPT_3	-.746	-2.196	.107	.158
Normative Pressures Participation in Associations	NPP_1	-.312	-.918	-.444	-.654
	NPP_2	-.257	-.756	-.385	-.566
	NPP_3	-.065	-.190	-.333	-.490
Normative Pressures Managers' Background	NPM_1	-.173	-.509	-.654	-.963
	NPM_2	-.337	-.992	-.584	-.859
	NPM_3	-.064	-.190	-.473	-.697
Adoption Intention	AI_1	-.448	-1.320	-1.199	-1.765
	AI_2	-1.001	-2.948	-.037	-.054
	AI_3	-.759	-2.235	-.585	-.862
Multivariate				**28.023**	**2.042**

[7] C.R. is abbreviated from "Critical Ratio".

After examinations of reliability, validity, and multivariate normality, the analysis processes can move further to the structural equation modeling and hypotheses testing.

5.3.2 Model Fitting and Hypotheses Testing

As theoretical foundations supported the model under study, it was appropriate to evaluate the associations of the constructs with structural equation modeling (SEM), which is a technique for discovering potential latent structures (Jöreskog & Sörbom, 1993). The research model was tested using SEM techniques, and the performed by AMOS 18.0.0 (Build 992). The estimation procedure used was Maximum Likelihood (ML). The ML estimator performs relatively well under several conditions (Hoyle & Panter, 1995), it assumes normality of the data, and the univariate normality for each variable and the multivariate normality were tested in previous section.

The term “structural” indicates that the parameters are not just descriptive measures of association but rather that they reveal a invariant “causal” relation (Bollen, 1989). The advantages of structural equation modeling is that it is a statistical technique that examines a series of multiple interrelated dependence relationships simultaneously, with the ability to represent unobserved concepts in these relationships and account for the measurement error in the estimation process (Hair, et al., 1995). In effect, this comprehensive means of assessing and modifying theoretical models offer great potential for furthering theory development (Anderson & Gerbing, 1988).

Measures of Model Fit

Fit indices provide a relative sense of the fit of the model studied, although referred to as “goodness-of-fit (GOF)”, they often are a measure of non-fit. Each index has various strengths and weaknesses, and therefore most researchers report multiple indices for contemplation. Tanaka (1993), Maruyama (1997), and others distinguish between several types of fit indices:

1. **Absolute fit indices:** the absolute fit indices are simply derived from the fit of the obtained and implied covariance matrices and the ML minimization function rather than using an alternative model as a base for comparison. The absolute fit indices include chi-square (χ^2) with corresponding p-value, Goodness of Fit Index (GFI), Adjusted GFI, Hoelter's CN, Akaike information criterion (AIC), Bayes information criterion (BIC), Expected Cross-Validation Index (ECVI), the root mean square error of approximation (RMSEA) and root mean square residual (RMR).
2. **Relative fit indices:** Relative fit indices compare a chi-square for the tested model to one from a null model (also called a "baseline" model or "independence" model). The null model is a model tested that specifies that all measured variables are uncorrelated. The relative fit indices such as the comparative fit index (CFI), Bollen's (1989) incremental fit index (IFI), Tucker-Lewis coefficient index (TLI), and Bentler-Bonett (1980) normed fit index (NFI) are often seen in the literature.
3. **Parsimony fit indices:** The parsimony fit indices are relative fit indices that are adjustments to the relative fit indices above. The simpler theoretical processes are favored over more complex ones, so that the adjustments are to penalize models that are less parsimonious. The more complex the model, the lower the fit index, and such indices including PGFI, PNFI, and PCFI (the "P"s are abbreviated from "parsimony adjustment").

The most common fit measures include the chi-square (χ^2) with degrees of freedom (df) and a p-value, the root mean square error of approximation (RMSEA), the comparative fit index (CFI), normed fit index (NFI) and parsimony adjustments to the CFI (PCFI) and NFI (PNFI). We thereby selected these indices as our model evaluation guidelines, and these indices will be discussed in more detailed manner in following paragraphs. These indices covered all types of indices mentioned earlier, and they could provide a comprehensive evaluation of our model.

Chi-square (χ^2); although of referred to as a test statistic, in SEM, the chi-square is more of a assessment of fit, measuring the distance between the sample covariance matrix and the fitted covariance matrix. A large chi-square indicates the model fitting is bad, since the chi-square is representing how much the data is to be apart from the model. Hence, a non-significant chi-square value is desired, and one attempts to infer the validity of the hypothesis of no difference between the collected data and proposed model (the model to be tested) (Bentler & Bonett, 1980). The drawback with chi-square as a fit measure it its relation to sample size, the value could be very large while the sample size increases. McDonald and Marsh (1990) addressed that while the sample size increases, the model will be rejected by the asymptotic chi-square test at any fixed level of significance. The large of a sample generates to large chi-square value to reject the proposed model. Therefore, many researchers used the ratio of chi-square to degrees of freedom (CMIN/df) instead. The ratio of chi-square values over the degrees of freedom (CMIN/df) was one of the earliest criteria designed to be less sensitive than the chi-square sample size. It could be said to be a normalization of chi-square (Blunch, 2008). Where this ratio value is less than 3, it indicates good model fit (Schumacker & Lomax, 2004).

Root Mean Square Error of Approximation (RMSEA) is a measure of discrepancy per degree of freedom. The RMSEA could be said to be a “badness of fit” criteria, with lower scores reflecting better fit. RMSEA values less than 0.06 indicate very good fit (Hu

& Bentler, 1999), values between 0.06 to 0.08 indicate good fit, while values ranging from 0.08 to 0.10 indicate fair fit (Byrne, 2006).

CFI; the comparative fit index (CFI) compares the hypothesized model to the independence model, rescaling the chi-square into a zero to 1.00 range, with 1.00 indicating perfect fit (Byrne, 2006), and it takes degrees of freedom into consideration (Blunch, 2008). CFI was chosen because of its resistance to the effects of sample size. In general, CFI should be equal to or greater than 0.90 for the model to be accepted (Hu & Bentler, 1999).

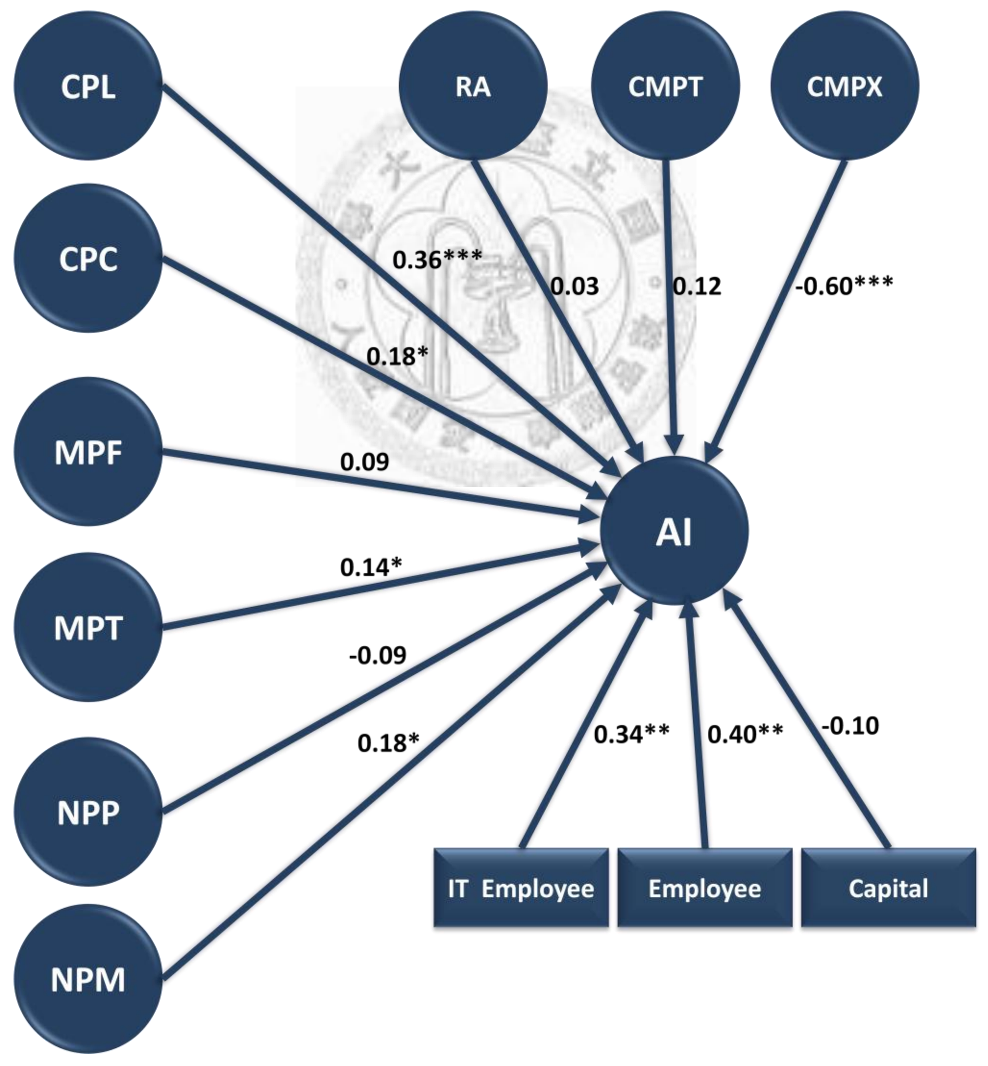
NFI; the normed fit index (NFI) was proposed by Bentler and Bonett (1980). They claimed the index are independent of sample size and suggested that the measure can be applied to any fit function and employed with the maximum likelihood (ML) or generalized least squares (GLS) procedures. The value of NFI equal to or greater than 0.90 indicates the model is good fit.

PCFI /PNFI are the result of applying the parsimony adjustment to the CFI/PNFI (James, et al., 1982). The PCFI/PNFI are the CFI/NFI value multiplies the ratio of the degrees of freedom for the model being evaluated divided by the degrees of freedom for the baseline model. The measure represents an attempt to balance these two conflicting objectives - simplicity and goodness of fit. Therefore, the higher of PCFI/PNFI values indicate the model is more parsimonious and preferable, and their values should equal to or greater than 0.5 to indicate an adequate fit (Byrne, 2006; Hair, et al., 2006).

Model Fitting

The results of the tests performed and the model building were shown below. WE explored the relations among adoption intention and relative advantages (RA), compatibility (CMPT), complexity (CMPX), coercive pressures – legal requirements (CPL), coercive pressures – customers' requirements (CPC), mimetic pressure – frequency-based mimicry (MPF), mimetic pressure – trait-based mimicry (MPT), normative pressures – participation in profession associations (NPP), normative pressures – mangers' background (MPM), and several control variables (i.e., industry, capital, employees, IT department employees) in a structural model. Figure 5-1 clearly illustrated the hypothesized structure model and corresponding path coefficients.

Figure 5-1: Results of the Full Structural Model



The model proposed by the study revealed a moderate fit to the given data, and the goodness-of-fit (GOF) indices we used in the study were shown in table 5-6. The reported goodness-of-fit measures reveal chi-square value of 1134.54 with 484 degrees of freedom at p=0.000 level of significance, representing the model was not fitting well with the data. However, just mentioned earlier, the chi-square is not a good index for evaluating the goodness-of-fit, so we divided chi-square by its degrees of freedom to get the CMIN/DF value of 2.344, which fell into the suggested value, representing the proposed model had a good fit. Another one absolute fit index used to evaluate the model is RMSEA, which the value as 0.162, and it’s slightly higher than the suggested criterion of 0.1, therefore we inferred our model was a moderate fit indicated by RMSEA. The absolute model fit indices were quite acceptable, but the relative indices (i.e., CFI and NFI) indicated the model was inadequate, both of the indices were fell below the criterion (CFI = 0.687 < 0.9 and NFI = 0.564 < 0.9). For the parsimony indices, including PCFI and PNFI, revealed that the model is adequate (PCFI = 0.629 > 0.5, PNFI = 0.517 > 0.5).

Generally speaking, from all the three types of GOF indices, we could say that our proposed model had a moderate goodness of fit to the collected data. Why the model was not fitted well? The possible reasons that might cause such problems will be discussed later in the discussions. Given the model was moderate fitted; we can examine the path coefficients and test our hypotheses.

Table 5-5: Fit Indices of the Proposed Model

GOF index	Default Model[8]	Saturated model	Independent model	Criterion
Chi-Square	1134.54	N/A	2603.62	P-value ＞ 0.05
Degrees of Freedom	484		528	
P-value	0.000		0.000	
CMIN/DF	2.344	N/A	4.931	＜ 3
RMSEA	0.162	N/A	0.272	＜ 0.1
CFI	0.687	1.000	0.000	＞ 0.9
NFI	0.564	1.000	0.000	＞ 0.9
PCFI	0.629	0.000	0.000	＞ 0.5
PNFI	0.517	0.000	0.000	＞ 0.5

Hypotheses Testing

The SEM analysis provided the path coefficient result that we used to analyze the hypotheses. Table 5-5 reported the detail estimates of path coefficient values for each factors. We found that adoption intention was significantly influenced by several factors at the significant level of 0.05. The significant factors included the complexity of ISO 27001 (with the parameter estimate = -0.600 and p-value less than 0.001), coercive pressures – legal requirements (parameter estimate = 0.364 and p-value less than 0.001), coercive pressures – customers' requirements (parameter estimate = .186 and p-value = 0.012), mimetic pressures – trait-based mimicry (parameter estimate = .157 and p-value = 0.032), normative pressures – managers' background (parameter estimate = .170 and p-value = 0.017), and two control variables (including number of company employees and number of employees in IT department).

[8] Default model is the model we proposed and wanted to test.

Table 5-6: Path Coefficient Results

			Standardized Estimate	Estimate	S.E.	C.R.	P-value[9]
AI	←	RA	0.030	0.028	0.070	0.403	0.687
AI	←	CMPT	0.115	0.109	0.071	1.540	0.123
AI	←	CMPX	-0.603	-1.954	0.583	-3.353	***
AI	←	CPL	0.357	0.355	0.079	4.497	***
AI	←	CPC	0.180	0.163	0.068	2.392	0.017
AI	←	MPF	0.087	0.085	0.075	1.138	0.255
AI	←	MPT	0.144	0.143	0.073	1.951	0.047
AI	←	NPP	-0.093	-0.106	0.080	-1.336	0.182
AI	←	NPM	0.177	0.254	0.105	2.422	0.015
AI	←	capital	-0.095	-0.043	0.053	-0.821	0.411
AI	←	employee	0.397	0.250	0.080	3.131	0.002
AI	←	IT_employee	0.341	0.204	0.077	2.665	0.008

From the SEM analysis results, the nine hypotheses we proposed were tested in this study, each tested the associations between the ISO 27001 adoption intention and the possible influencing variables. Table 5-7 summarized the hypotheses testing results. For the control variables, two control variables used in the model have significant impact on the adoption intention, including the number of organization employees (parameter = 0.397 and p-value = 0.002) and IT department employees (parameter = 0.341 and p-value = 0.008), and the results are consistent with past research (Damanpour, 1991; Rogers, 2003; Teo, et al., 2003; Zmud, 1984). The last one control variable (i.e., capital) has no significant influence on the intention, indicating the adoption intention is less influenced by their capital while other variables are already taken in considerations.

[9] *** indicates the value was less than 0.001 and it could not be shown by the software.

Table 5-7: Summary of Hypotheses Testing Results

Hypothesis	Descriptions	P-value[10]	Supported
H_1 (+)	Greater perceived relative advantage of ISO27001 the more likely they will be adopted.	0.687	No
H_2 (+)	Greater perceived compatibility of ISO 27001 with current business processes, the more likely they will be adopted.	0.123	No
H_3 (–)	Greater perceived complexity of ISO 27001 the less likely they will be adopted.	***	Yes
H_{4a} (+)	Greater perceived pressures of legal requirements results in greater adoption intention of ISO 27001.	***	Yes
H_{4b} (+)	Greater perceived pressures of customer requirements results in greater adoption intention of ISO27001.	0.017*	Yes
H_{5a} (+)	Greater extent of adoption of ISO27001 among its competitors will results in greater adoption intention of ISO27001.	0.255	No
H_{5b} (+)	Greater number of successful organizations that adopted ISO 27001 results in greater adoption intention of ISO27001.	0.047*	Yes
H_{6a} (+)	The more active participations of an organization in professional and trade associations results in greater adoption intention of ISO27001.	0.182	No
H_{6b} (+)	Greater similarity of managers' background results in greater adoption intention of ISO27001.	0.015*	Yes

5.4 Discussions

This section reviews the findings from previous results and discusses the possible reason from literature and practices perspectives. Hypotheses 1 to 3 are regarding the relationship between adoption intention and the characteristics of innovation (i.e., ISO

[10] * significant at the alpha = 0.05 level
** significant at the alpha = 0.01 level
*** significant at the alpha < 0.001 level (the exactly value could not be shown by the software.)

27001 or ISMS) from the diffusion of innovation theory.

Hypothesis 1 asserts that the greater perceived relative advantage of ISO 27001 were expected to result in higher likelihood of adoption, but the testing results showed that it did not significantly influence the adoption intention. In the meta-analysis of Tornatzky and Klein’s research (1982), they analyzed 29 studies that used the characteristic of relative advantage, and found only 11 reported statistical results directly relevant to the relationship of the relative advantage of an innovation to its adoption. Moreover, in the study of multimedia message service (MMS) adoption by Hsu et al. (2007), they found that there are existing differences between user groups, the relative advantage significantly affects intention to use for the innovators, early-adopters, early-majority, and late majority groups. However, for the laggards, there are no significant relationships were found. This may raise an indication that, for the organizations that are early adopters, the adoption of innovation are driven by the relative advantages, but for the laggards, they might driven by other factors. This might cause the relative advantages to be no significances. Another possible reason is that, in Taiwan, the government agencies, universities, hospitals, and finance industry are receiving more legal pressures; and for the large technologies and manufacturing organizations, they need to comply not only comply with regulations and customers’ of Taiwan, they also have to comply with regulations and customers abroad. Hence, for the organizations, they adopt ISO 27001 because of the coercive pressure rather then they perceived the advantages of ISO 27001.

Hypothesis 2 asserts that the greater perceived compatibility of ISO 27001 with current business processes, the more likely they will be adopted. In our study, the link between organizational compatibility with ISO 27001 and the intention of ISO 27001 adoptions was not strong enough to be significant. Even through the compatibility should be an important factor for the adoption (Tornatzky & Klein, 1982), several studies in their analysis still showed non-significance of compatibility, and in recent studies, compatibility might not be significant (Hsu, et al., 2007; O'Callaghan, et al., 1992). We believe that compatibility of ISO 27001 was not significant, because the organizations somewhat need to ignore the incompabilities and adopt the innovation while they perceived large pressure. Moreover, there are many organizations even do not realized how the adoption and implementation of ISO 27001 will change their processes. In consideration of the significance level of compatibility ($\alpha = 0.123$) was close to be significant, it also reveals the implications that they might not quite clear whether ISO 27001 will change the process. Hence, we suggest that the influences of compatibility should be more carefully studied in future research.

Hypothesis 3 postulates that the organizations will less likely adopt ISO 27001 while they perceived greater complexity of ISO 27001. The testing results showed the relationship between complexity and adoption intention was significant, and it was conformed with our hypothesis. That means, while the adopters consider the ISO 27001 is too complexity for their organizations, they will less likely adopt ISO 27001 and maybe seek another similar standard if an ISMS is necessary. Another notable is that we only ask the respondents whether they perceived the ISO 27001 is complex or not, we did not clarify the perceived complexity between the adoption and certification process, some organization might use the essence of ISO 27001 but did not certificate them. The complexity that potential adopter perceived is due to the adoption and implementation process, or it is due to the certification process should be discriminated in the future studies.

Hypotheses 4_a to 6_b are regarding the association between adoption intention and intuitional pressures the organizations perceived.

Hypotheses 4_a and 4_b claim that the coercive pressures are positively related to the adoption intention of ISO 27001. The results indicated there was a strong relationship among coercive pressures – legal requirements and adoption intention (hypothesis 4_a). The organizations that influenced by the laws or regulations had to adopt ISO 27001 inevitably, they could not resist such pressures. On the other hand, the coercive pressures – customers' requirements (hypothesis 4_b) was also significant, revealing that the organizations will adopt ISO 27001 in order to maintain a business relationship with their customers. The two hypotheses (4_a and 4_b) results indicate the coercive pressures play an important role that drive the organizations to adopt ISO 27001. The organizational decision makers have a greater tendency to comply with the laws and regulation and their customers' requisitions. These findings are consistent with several researches of different area. For example, Khalifa and Davison (2006) found that the customers' pressures have significant influence on the intention of small and medium-sized enterprises (SME) brokerages to adopt electronic trading systems (ETS), and Teo et al. (2003) also found the customers could influence organizational predisposition toward an information technology-based inter-organizational linkage

Hypotheses 5_a and 5_b anticipate that the mimetic pressures are positively related to the intention of ISO 27001 adoptions. However, only the trait-based mimicry (i.e., hypothesis 5_b) was significant, representing the organizations selectively imitate practices that have been used by subset of other organizations (usually large and successful organizations) (Haunschild & Miner, 1997) and seek for acquiring higher status by imitating the leading organizations (Fombrun & Shanley, 1990). Another proposition, the frequency-based mimicry (hypothesis 5_a), has failed to be supported by the analysis.

Guler et al. (2002) have shown that the behavior of intuitional mimicry was observed in the case of ISO 9000, however, the effect may be less important at first because of the initially low number of adopter in each country of the case of ISO 14001 (Delmas, 2002). We believe that there exists the same circumstances for ISO 27001, and the organization decision makers selectively imitate the leading companies rather the extent of the innovation.

Hypotheses 6_a and 6_b proposes that the greater perceived normative pressures results in higher intention to adopt ISO 27001. The hypothesis 6_b was supported but the hypothesis 6_a was not supported. Actually, some of the respondents told us that they were not sure whether their organizations were actively participating the trade or professional association which promoting ISO 27001. From our collected data also showed that almost 70% of the responses of the construct items were slightly agree, neither agree nor disagree, or slightly disagree, indicating the respondents were not quite sure the attitude about ISO 27001 of the associations they participated. Another possible reason why the proposition was not hold is the organization may also be exposed to negative information (e.g., the cost or risks of adoption) through their participation in associations (Teo, et al., 2003). The result of another proposition (H_{6b}) comply with our assertions, exhibiting the decision makers (managers) who had security related background will more likely adopt ISO 27001. The possible reason is they know the importance of information security and regard it is crucial to their organization, and therefore they have higher intention to improve the information security management.

Overall, there was a strong empirical support for institutional-based variables as predictors of adoption intentions for ISO 27001, but for the innovation characteristics variables, only complexity showed the explanatory power. The institutional factors exhibit a significant and high influence on intentions to adopt ISO 27001 and the legal requirement is most powerful factor that impact on the intentions. The results were consistent with institutional and innovation diffusion theories, the evidence indicated that the innovation characteristics and institutional influences (i.e., complexity, mimetic pressures, coercive pressures, and normative pressures) can be clearly distinguished conceptually and empirically in terms of their influences on organizational predisposition toward ISO 27001.

Chapter 6 Conclusion

6.1 Implications for theory and practice

For the academics, we borrowed and combined two theories form the past research to predict the adoption intention. The combinations of the innovations diffusion theory and institutional theory can predict the intention more exhaustively, since the intention is influenced by many factors and too complex to be predicted by single theory, especially in the circumstances are not clear. In addition, while the institutional environments are not clear, drawing the insights of innovation diffusion theory to replenish the perspective of institutional theory is more appropriate for studying the adoption intention. By combining the two perspectives, we identified nine key constructs for analyzing the adoption intention of ISO 27001, although several constructs are not statistical significant, some constructs showed the influences on the adoption intention. Hence, from the theoretical inferences and the empirical test in above chapters, the diffusion of innovation and institutional theory should both be suitable for studying ISO 27001 adoptions, yet the further examinations of the innovation diffusion theory may still needed in future research. We apply the two theories to the area of information security and such an extension provides some new insights to the academics.

For the practices, even though the model could not be fitted well with our data, but there are still several constructs that found to be significant influencing the adoption intentions and these constructs can provide the managers a framework while considering the adoption. From the manager’s or potential adopter’s perspectives, the findings of the direct effect of innovation characteristics and institutional forces suggest that decision making is affected by outside compelling pressure, imitation, with or without conscious knowledge of it. Imitating others is not necessarily a disadvantage; sometimes it can bring second-mover advantages and be beneficial to the company. The decision makers have to be aware of the presence of these forces and the consequences they can bring, so that a suitable judgment can be made that leads to the maximization of returns for the company. The intuitional forces (especially the coercive pressures and trait-based mimicry) can help ISO 27001 accreditation service provider or consultants encourage the organizations to adopt ISO 27001. In addition to promoting ISMS, more efforts have to be made on reducing the complexity the potential adopter perceived. Efforts such as training courses, cultivating the security experts, advertising the basic knowledge of security and security issues can help the public to understand information security, and thus reducing the complexity they perceived.

6.2 Limitations and Suggestions for future research

This study has several notable limitations that should be addressed or considered for future research.

One of the major limitations of our study is the small sample size. Information security research is an intrusive types of organization research and hence it is hard to gain data from the organizations (Kotulic & Clark, 2004). In our sample collecting process, we faced many difficulties. The major problem is the organizations are unlikely to divulge information to outsiders without strong assurances that the information provided will in no way harm them. The small size of our sample thus restricts the generalizability and credibility of our study. The lack of time and resources cause such problems. Thus, for the future research, we suggest that it must be spending more time on the questionnaire distribution and collecting process, and seek for a reliable method to collect the data rather than online questionnaire, which is considered to be unsecure. We believe that more and reliable data can be gathered with such ameliorations.

Second, since this study was conducted in Taiwan, the generalizability of our results is limited to the organizations of Taiwan and those in similar institutional contexts. While generalizing these findings to organizations operating in different institutional and cultural environments, several cautions must be aware, such as level of complexity perceived or different law and regulation requirements in the global. For example, the SOX and Basel II are important regulations for US companies to comply with, so the coercive pressures should be a significant factor. The number of certification registers may also cause the extent of mimetic forces, for instance, more than 3000 ISO 27001 registers are Japan organizations and the visibility of ISO 27001 should be greater than other countries. Therefore the mimetic pressures are enforced, causing the organizations are more likely to mimic their competitors. For the future research, the differences of institutional and cultural environments between countries should be carefully examined while using institutional and innovation diffusion theories.

Third, although the adoption intention positively related to the actually adoption is undoubted, they are not identical. That means higher intention results higher possibility of adoption, but it may not results actually adoption definitely. However, the question whether the organization with high intention will actually adoption ISO 27001 is related to a longitudinal data collection and analysis, it is hard to be conducted in our study due to the time and resources was restricted. Therefore, for the further research, it would be more better answer the question why the organization adopt an innovation by carrying out a longitudinal investigations of these organizations. We believe that, by studying the organizations with high adoption intention but not actually adopt, it could provide valuable information and insights regarding the diffusion of innovations. A longitudinal investigation would be an appropriate approach to address this timing issue.

6.3 Concluding Comments

Since the importance of information security and its severe impacts on organizations, the improvement of information security controls as well as managements are crucial for all organizations. For the information security management, ISO 27001 is the most important standards and it plays an important role while the organizations are considering strengthening their security management. However, with so many publications talking about the ISO 27001, there are scanty of academic researches focus on the ISO 27001 issues and nearly no researches were studying the adoption intentions of ISO 27001.

The ISO 27001 is a prominent standard of information security management, yet there is lack of academic attentions. Such deficiencies of the literature should be addressed, hence our research focused on the adoption intention of ISO 27001 in the extent of Taiwan, where the number of adoption organizations is listed at the 4th among the global[11]. In a small country but with high adoption rate of ISO 27001, it is an appropriate circumstance for studying what driver the organizations to adopt ISO 27001.

Before examine the adoption intentions, we need to know what is inside ISO 27001 and what are the characteristics of ISO 27001, knowing the nature of it is necessary for studying it. Therefore, we regards the ISO 27001 (or ISMS) is an administrative innovation, since the nature of ISO 27001 conformed to the traits of administrative innovations (Hsu, et al., 2010). From the innovation literatures, we introduced two important (i.e., innovation diffusion theory (Rogers, 2003) and institutional theory (DiMaggio & Powell, 1983)) theories, both were widely used while studying adoption intentions, to the studies of ISO 27001. Combining the merits of two theories, we identified nine factors that might make influences on the intention of adoption and tested

[11] See http://www.iso27001certificates.com/ for detail numbers, the rank we accessed on June 18, 2010.

those factors. From the innovation diffusion theory, we found the complexity exhibits the significant influences on intentions. From the perspective of institutional theory, the institutional environments are important influencing factors for organizations. Especially the coercive pressures, the organizations have no choice but to comply with the laws, regulations, and their essential customers' requisitions.

The adoption intentions could be explained by the lens of the integrated model, and the findings filled the lack of studies on the ISO 27001 adoption. This study provides several academic and practical implications. It also extended the empirical literature of institutional and innovation diffusion studies to the area of information security. This study has several limitations as with any social science research, but, notwithstanding the defects and limitations, our study is one of the few that examines the importance of innovation characteristics and institutional environments simultaneously on the diffusion of innovation.

We hope the defects and limitations of our study can further be overcome in the future research, and thus to be more well-understanding the adoption intentions and behaviors. We believe the more conversant with intentions will lead us to be more understanding with the organizational behavior.

References

Adams, D., Nelson, R., & Todd, P. (1992). Perceived usefulness, ease of use, and usage of information technology: a replication. *MIS Quarterly, 16*(2), 227-247.

Anderson, J., & Gerbing, D. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin, 103*(3), 411-423.

Attewell, P. (1992). Technology diffusion and organizational learning: The case of business computing. *Organization science, 3*(1), 1-19.

Basel, II. (2004). Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework: Basel Committee Publications.

Bentler, P. (2006). *EQS 6 structural equations modeling program manual.* California: Multivariate Software.

Bentler, P., & Bonett, D. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological bulletin, 88*(3), 588-606.

Bidgoli, H. (2006). *Handbook of Information Security Volume 1-3*. New Jersey: John Wiley & Sons.

Bjorck, F. (2004). *Institutional theory: a new perspective for research into IS/IT security in organisations.* Paper presented at the The 37th Annual Hawaii International Conference on Information Systems 2004 (HICSS'04).

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management.* Paper presented at the workshop on New security paradigms.

Blunch, N. (2008). *Introduction to structural equation modelling using SPSS and AMOS*. California: Sage.

Bodin, L., Gordon, L., & Loeb, M. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64-68.

Bollen, K. (1989). *Structural equations with latent variables*. New Jersey: John Wiley &

Sons.

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk Management Magazine, 54*, 24-29.

Byrne, B. (2006). *Structural equation modeling with EQS: Basic concepts, applications, and programming*. New Jersey: Lawrence Erlbaum Associates.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28-46.

Cerullo, V., & Cerullo, M. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management, 21*(3), 70-78.

Chatterjee, D., Grewal, R., & Sambamurthy, V. (2002). Shaping Up For E-Commerce:Institutional Enables of The Organisational Assimilation Web Technologies. *MIS Quarterly, 26*(2), 65-89.

Chen, A., Watson, R., Boudreau, M., & Karahanna, E. (2009). *Organizational Adoption of Green IS & IT: An Institutional Perspective.* Paper presented at the 30th IInternational Conference on Information Sytems (ICIS 2009), Phoenix.

Chen, T., Chung, Y., & Huang, G. (2003). Efficient proxy multisignature schemes based on the elliptic curve cryptosystem. *Computers & Security, 22*(6), 527-534.

Chin, W., & Gopal, A. (1995). Adoption intention in GSS: relative importance of beliefs. *ACM SIGMIS Database, 26*(2&3), 42-64.

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73.

Cooper, R., & Zmud, R. (1990). Information technology implementation research: a technological diffusion approach. *Management Science, 36*(2), 123-139.

Cronbach, L. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,* *16*(3), 297-334.

Culnan, M. J., & Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. *MIS Quarterly, 33*(4), 673-687.

D'Arcy, J., & Hovav, A. (2008). An Integrative Framework for the Study of Information Security Management Research. In J. N. D. Gupta & S. K. Sharma (Eds.), *Handbook of Research on Information Security and Assurance* (pp. 55-67). Pennsylvania: IGI Global.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

Damanpour, F. (1991). Organisational Innovation: A Meta-Analysis of Effects of Determinants and Moderators. *Academy of Management Journal, 34*(3), 555-590.

Damanpour, F. (1992). Organizational size and innovation. *Organization studies, 13*(3), 375.

Delmas, M. (2002). The diffusion of environmental management standards in Europe and in the United States: an institutional perspective. *Policy Sciences, 35*, 91-119.

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organisational Perspectives. *Information Systems Journal, 11*(2), 127-153.

Dickerson, M., & Gentry, J. (1983). Characteristics of adopters and non-adopters of home computers. *Journal of Consumer Research, 10*(2), 225-235.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organisational Fields. *American Sociological Review, 48*(2), 147-160.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2008). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Downs Jr, G., & Mohr, L. (1976). Conceptual issues in the study of innovation. *Administrative Science Quarterly, 21*(4), 700-714.

DTI/PWC. (2008). *Safeguarding the new currency of business - Findings from the 2008 Global State of Information Security Study*.

E&Y. (2008). *Moving beyond compliance - Ernst & Young's 2008 Global Information Security Survey*.

Eloff, J., & Eloff, M. (2003). *Information security management: a new paradigm.* Paper presented at the annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.

Ezingeard, J., & Birchall, D. (2005). *Information security standards: Adoption drivers (invited paper)*. Paper presented at the Security management, integrity, and internal control in information systems.

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., & Weippl, E. (2007). *Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard.* Paper presented at the 13th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'07), Victoria.

Fischer, P. (2007). Security Evaluation and Testing Past, Present and Future. In Sacher Paulus, Norbert Pohlmann & H. Reimer (Eds.), *ISSE 2004 - Securing Electronic Business Processes: Highlights Of The Information Security Solutions Europe 2004 Conference* (pp. 322 -328): Vieweg.

Fombrun, C., & Shanley, M. (1990). What's in a name? Reputation building and corporate strategy. *Academy of Management Journal, 33*(2), 233-258.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Frost, P., & Egri, C. (1991). The political process of innovation. *Research in organizational behavior, 13*, 229-245.

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management, 26*(2), 128-141.

Gopal, R., & Sanders, G. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13*(4), 29-47.

Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.

Guler, I., Guillen, M., & Macpherson, J. (2002). Global Competition Institutions, and the Diffusion of Organsational Practices: The International Spread of ISO 9000 Quality Certificates. *Administrative Science Quarterly, 47*(2), 207-223.

Gupta, B. B., Joshi, R. C., & Misra, M. (2009). *An efficient analytical solution to thwart DDoS attacks in public domain.* Paper presented at the International Conference on Advances in Computing, Communication and Control.

Gupta, J., & Sharma, S. (2008). *Handbook of Research on Information Security and Assurance*. Pennsylvania: Information Science Reference.

Gupta, M., & Sharman, R. (2009). *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Pennsylvania: Information Science Reference.

Hair, J., Anderson, R., Tatham, R., & Black, W. (1995). *Multivariate data analysis: with readings*. New Jersey: Prentice-Hall.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis*. New Jersey: Prentice Hall.

Harn, L., & Ren, J. (2006). Efficient identity-based RSA multisignatures. *Computers & Security, 27*(1-2), 12-15.

Haunschild, P., & Miner, A. (1997). Modes of Interorganizational Imitation: The Effects of Outcome Salience and Uncertainty. *Administrative Science Quarterly, 42*(3), 472-500.

Hawley, A. H. (1986). *Human ecology: A theoretical essay*. Chicago: University of Chicago Press.

Hoyle, R., & Panter, A. (1995). Writing about structural equation models. In R. H. Hoyle (Ed.), *Structural equation modeling: Concepts, issues, and applications* (pp. 158-176). California: : Sage.

Hsu, C., Lee, J.-N., & Straub, D. W. (2010). Institutional Influences on Information Security Innovations. *Working paper*.

Hsu, C., Lu, H., & Hsu, H. (2007). Adoption of the mobile Internet: An empirical study of multimedia message service (MMS). *Omega, 35*(6), 715-726.

Hu, L., & Bentler, P. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: adoption and impact of technology. *MIS Quarterly, 19*(4), 465-485.

ISO, B. S. (2005a). ISO/IEC 27001: 2005, *Information Technology - Security Techniques - Information Security Management Systems - Requirements*.

ISO, B. S. (2005b). ISO/IEC 27002: 2005, *Information Technology. Security Techniques.*

Code of Practice for Information Security Management.

ISO, B. S. (2008). ISO/IEC 27005: 2008, *Information Technology - Security Techniques - Information Security Risk Management*.

Jöreskog, K., & Sörbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Illinois: Scientific Software.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security, 1*(2), 125-143.

James, L., Mulaik, S., & Brett, J. (1982). *Causal analysis: Assumptions, models, and data*. New Jersey: Sage.

Jeyaraj, A., Balser, D., Chowa, C., & Griggs, G. (2009). Organizational and institutional determinants of B2C adoption under shifting environments. *Journal of Information Technology, 24*(3), 219-230.

Khalifa, M., & Davison, M. (2006). SME adoption of IT: the case of electronic trading systems. *IEEE Transactions on Engineering Management, 53*(2), 275-284.

Kimberly, J., & Evanisko, M. (1981). Organisational Innovation: The Influence of Individual, Organisational, and Contextual Factors on Hospital Adoption of Technological and Administrative Innovations. *Academy of Management Journal, 24*(4), 689-713.

Kline, R. (2005). *Principles and practice of structural equation modeling*. New York: The Guilford Press.

Knapp, K. (2009). *Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions*. Pennsylvania: Information Science Reference.

Knight, K. E. (1967). A descriptive model of the intra-firm innovation process. *Journal of Business, 40*, 478-496.

Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Lai, V., Liu, C., Lai, F., & Wang, J. (2008). *Examining ERP Committee Beliefs: A Comparison of Alternative Models*. Paper presented at the International Conference on Information Systems (ICIS) 2008.

Li, M. (2006). Change trend of averaged Hurst parameter of traffic under DDOS flood attacks. *Computers & Security, 25*(3), 213-220.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS Quarterly, 31*(1), 59-87.

Lyytinen, K. (1991). Penetration of information technology in organizations: A comparative study using stage models and transaction costs. *Scandinavian journal of information systems, 3*(1), 87-109.

Mambo, M., Usuda, K., & Okamoto, E. (1996). *Proxy signatures for delegating signing operation.* Paper presented at the 3rd ACM conference on Computer and communications security, New Delhi.

March, J. (1981). Decisions in organizations and theories of choice. In A. H. Van de Ven & W. F. Joyce (Eds.), *Perspectives on organization design and behavior* (pp. 205-244). New York: John Wiley & Sons Inc.

Mardia, K. (1970). Measures of multivariate skewness and kurtosis with applications. *Biometrika, 57*(3), 519-530.

Mardia, K. (1974). Applications of some measures of multivariate skewness and kurtosis in testing normality and robustness studies. *Sankhy : The Indian Journal of Statistics, Series B, 36*(2), 115-128.

Maruyama, G. (1997). *Basics of structural equation modeling*. New Jersey: Sage Publications.

McDonald, R., & Marsh, H. (1990). Choosing a multivariate model: Noncentrality and goodness of fit. *Psychological bulletin, 107*(2), 247-255.

Mellado, D., Fernández-Medina, E., & Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces, 29*(2), 244-253.

Meyer, A., & Goes, J. (1988). Organizational assimilation of innovations: a multilevel contextual analysis. *Academy of Management Journal, 31*(4), 897-923.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American journal of sociology, 83*(2), 340-363.

Nunnally, J., & Bernstein, I. (1978). *Psychometric theory*. New York: McGraw-Hill.

Nunnally, J., Bernstein, I., & Berge, J. (1994). *Psychometric theory*. New York: McGraw-Hill

O'Callaghan, R., Kaufmann, P., & Konsynski, B. (1992). Adoption correlates and share effects of electronic data interchange systems in marketing channels. *Journal of Marketing, 56*(2), 45-56.

Plouffe, C., Hulland, J., & Vandenbosch, M. (2001). Richness versus parsimony in modeling technology adoption decisions--understanding merchant adoption of a smart card-based payment system. *Information Systems Research, 12*(2), 208-222.

Prescott, M. B., & Conger, S. A. (1995). Information technology innovations: a classification by IT locus of impact and research approach. *ACM SIGMIS Database, 26*(2-3), 20-41.

Ramamurthy, K., Sen, A., & Sinha, A. (2008). An empirical investigation of the key determinants of data warehouse adoption. *Decision Support Systems, 44*(4), 817-841.

Richardson, R. (2008). *CSI/FBI Computer Crime and Security Survey 2008*.

Rogers, E. M. (1995). *Diffusion of innovations*. New York: Free Press.

Rogers, E. M. (2003). *Diffusion of innovations*: New York: Free Press.

Rowe, L. A., & Boise, W. B. (1974). Organizational innovation: Current research and evolving concepts. *Public Administration Review, 34*(3), 284-293.

Schultz, E. E. (2004). Sarbanes-Oxley - a huge boon to information security in the US. *Computers & Security, 23*(5), 353-354.

Schumacker, R., & Lomax, R. (2004). *A beginner's guide to structural equation modeling*. New Jersey: Lawrence Erlbaum Associates.

Scott, W. R. (2001). *Institutions and organizations*. California: Sage.

Siponen, M., & Willison, R. (2007). *A critical assessment of IS security research between 1990-2004.* Paper presented at the 15th European Conference on Information Systems, St. Gallen, Switzerland.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38*(1), 60-80.

Smith, E., & Eloff, J. (2002). A Prototype for Assessing Information Technology Risks in Health Care. *Computers & Security, 21*(3), 266-284.

Son, J., & Benbasat, I. (2007). Organizational Buyers' Adoption and Use of B2B Electronic Marketplaces: Efficiency-and Legitimacy-Oriented Perspectives. *Journal of Management Information Systems, 24*(1), 55-99.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems*: NIST special publication.

Straub, D. W. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management, 26*(1), 2-12.

Sun, L., Srivastava, R., & Mock, T. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109-142.

Tan, M., & Teo, T. (2000). Factors influencing the adoption of Internet banking. *Journal of the AIS, 1*(1es).

Tanaka, J. (1993). Multifaceted conceptions of fit in structural equation models. In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 10-39). California: Sage.

Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144-176.

Teo, H., Tan, B., & Wei, K. (1995). *Innovation diffusion theory as a predictor of adoption intention for financial EDI.* Paper presented at the International Conference on Information Systems (ICIS).

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting Intention to Adopt Interorganisational Linkage: An Institutional Perspective. *MIS Quarterly, 27*(1), 19-49.

Teo, T., Lim, G., & Fedric, S. (2007). The adoption and diffusion of human resources information systems in Singapore. *Asia Pacific Journal of Human Resources, 45*(1), 44.

Tierney, J. (2008). Common Criteria A brief history and overview. In K. E. Mayes & K. Markantonakis (Eds.), *Smart Cards, Tokens, Security and Applications* (pp. 173-194). Berlin Springer.

Tipton, H., & Krause, M. (2007). *Information Security Management Handbook*. Florida: CRC Press.

Tornatzky, L., & Klein, K. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management, 29*(1), 28-45.

Tsipenyuk, K., Chess, B., & McGraw, G. (2005). Seven pernicious kingdoms: A taxonomy of software security errors. *IEEE Security & Privacy, 3*(6), 81-84.

Vacca, J. (2009). *Computer and information security handbook*. Massachusetts: Morgan Kaufmann.

von Solms, B. (2000). Information security- the third wave? *Computers & Security, 19*(7), 615-620.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376.

von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security, 7*(1), 50-57.

Wang, H., & Wang, C. (2003). Taxonomy of security considerations and software quality. *Communications of the ACM, 46*(6), 75-78.

Weingart, S. H. (Ed.). (2000). *Physical security devices for computer subsystems: A survey of attacks and defenses*.

West, S., Finch, J., & Curran, P. (1995). Structural equation models with nonnormal variables: Problems and remedies. In R. Hoyle (Ed.), *Structural Equation Modeling: Concepts, Issues, and Applications* (pp. 56–75). California: Sage.

Westphal, J., Gulati, R., & Shortell, S. (1997). Customisation or Conformity? An Institutional and Network Perspective on the Content and Consequences of TQM Adoption. *Administrative Science Quarterly, 42*, 366-394.

Whitman, M. E., & Mattord, H. J. (2008). *Principles of information security*. Massachusetts: Course Technology.

Xu, J., & Lee, W. (2003). Sustaining availability of web services under distributed denial of service attacks. *IEEE Transactions on Computers, 52*(2), 195-208.

Zhu, K., Dong, S., Xu, S., & Kraemer, K. (2006). Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems, 15*(6), 601-616.

Zmud, R. (1984). An examination of'push-pull'theory applied to process innovation in knowledge work. *Management Science, 30*(6), 727-738.

Zucker, L. (1977). The role of institutionalization in cultural persistence. *American Sociological Review, 42*(5), 726-743.

Appendix A. Researches on IS Security

Table A-1: Researches on IS Security Technologies

	C&S	ISS	IM&CS	I&M	MISQ	ISR	JIS	JMIS	ISJ	EJIS	JAIS	CAIS
Cryptography and Secure Communications	234	202	122	3	0	0	0	0	0	0	0	2
System, Software, and Data Security	80	229	6	2	0	3	0	1	2	0	0	1
Security Attacks and Malwares	93	156	26	0	0	1	2	0	0	1	0	2
Physical Security	13	57	0	0	0	0	1	1	0	0	0	1
Standards and Certifications	7	6	2	0	0	0	0	0	0	0	0	1
Total	**427**	**650**	**156**	**5**	**0**	**4**	**3**	**2**	**2**	**1**	**0**	**7**

Table A-2: Researches on IS Security Management

	C&S	ISS	IM&CS	I&M	MISQ	ISR	JIS	JMIS	ISJ	EJIS	JAIS	CAIS
Risk Management	34	36	29	3	3	2	1	2	0	2	1	4
Awareness, Behavior, or Education Issues	31	49	27	0	1	1	0	0	1	1	1	0
Legal or Ethical Issues	37	123	40	8	6	2	2	3	0	3	3	5
Security Management Standards and Plan	78	129	43	3	2	1	0	0	2	1	1	2
Business Continuity Planning/Management	5	20	17	0	0	0	1	0	0	0	1	4
Security Investment and Strategy	5	20	12	0	0	3	0	4	0	0	0	1
Audit and Assurance	9	13	0	0	0	1	3	0	0	0	0	3
Total	**199**	**390**	**168**	**14**	**12**	**10**	**7**	**9**	**3**	**7**	**7**	**19**

Table A-3: Survey Period and Survey Volumes and Issues

Journal	**C&S**	**I&M**	**MISQ**	**ISS**	**ISR**	**JIS**	**JMIS**	**ISJ**	**EJIS**	**IM&CS**	**JAIS**	**CAIS**
Period	1995 ~ 2010	1995 ~ 2010	1995 ~ 2010	1995 ~ 2010	1995 ~ 2009	1995 ~ 2010	1995 ~ 2010	1998 ~ 2010	1999 ~ 2010	1995 ~ 2010	2000 ~ 2010	1999 ~ 2010
Volume (Issue)	14(1) ~ 29(4)	28(1) ~ 47(3)	19(1) ~ 34(2)	3(4) ~ 19(2)	6(1) ~ 20(4)	9(1) ~ 24(1)	11(4) ~ 26(4)	8(1) ~ 20(3)	8(1) ~ 19(2)	3(1) ~ 18(1)	1(1) ~ 11(4)	1 ~ 26

Appendix B. Questionnaire Instruments

Relative Advantages

- Improvement of management (adapted from (Lai, et al., 2008))
  - 導入 ISO27001 認證可以改善公司對於資訊流的控管
  - 導入 ISO27001 認證可以增進公司管理，降低資安事件造成的衝擊
  - 導入 ISO27001 認證可以使公司成員在資訊安全上的權責更加清楚

Compatibility

- Compatible with current process (adapted from (Teo, et al., 2007; Zhu, et al., 2006))
  - ISO27001 認證的規範相容於目前公司的作業流程
  - 公司原先的作業流程已經包含資訊安全上的考量
  - 要將公司的流程與 ISO27001 認證的規範做整合是容易的

Complexity

- Complexity of the certification (adapted from (Ramamurthy, et al., 2008; Teo, et al., 2007))
  - ISO27001 認證的內容對我們公司的資訊人員來說是容易理解的
  - 導入 ISO27001 的過程當中，公司需要針對 ISO27001 的規範內容做許多教育訓練與宣導
  - 整體來說，導入 ISO27001 認證是一個非常複雜的過程

Coercive forces

- Legal requirements (adapted from (Liang, et al., 2007) & (Chen, et al., 2009))
  - 法規或主管機關要求我們採用 ISO27001 認證
  - 目前或是未來可以預期的法規促使我們採用 ISO27001 認證
  - 採用 ISO27001 認證可使我們公司符合法規上對資訊安全的要求
- Customer requirements (adapted from (Khalifa & Davison, 2006))

- 我們的客戶認為我們應該採用 ISO27001 認證
- 為了與現有的客戶持續生意上的往來，我們須具備 ISO27001 認證
- 我們重要的大客戶鼓勵我們採用 ISO27001 認證

Mimetic forces

- Frequency-based imitation (adapted from (Son & Benbasat, 2007))
  - 許多與我們相同產業中的公司已經採用 ISO27001 認證
  - 許多我們產業中的公司在最近將會採用 ISO27001 認證
  - 我們的主要競爭對手已經採用 ISO27001 認證
- Trait-based imitation (adapted from (Lai, et al., 2008))
  - 採用 ISO27001 認證的公司通常是我們產業中規模較大的公司
  - 採用 ISO27001 認證的公司通常是我們產業中的領導公司
  - 採用 ISO27001 認證的公司通常是我們產業中非常成功的公司

Normative forces

- Participations in professional associations (adapted from (Son & Benbasat, 2007))
  - 許多壓力促使我們公司參與外界的協會與團體，而這些協會或團體皆推廣 ISO27001 認證
  - 我們積極的參與產業、商業或專家協會團體，而這些協會或團體皆推廣 ISO27001 認證
  - 我們經常關注於推廣 ISO27001 認證的協會或團體
- Managers' background
  - 我們產業中擁有資訊安全背景的管理者很少(例如有資訊安全相關認證、CISA、CISSP、或 ISO27001 Lead Auditor 等)
  - 我們資訊部門當中的許多管理者有資訊安全的背景(例如有資訊安全相關認證、CISA、CISSP、或 ISO27001 Lead Auditor 等)
  - 其他公司的資訊部門中，許多管理者有資訊安全的背景(例如有資訊安全

相關認證、CISA、CISSP、或 ISO27001 Lead Auditor 等）

Attitude & Intention (adapted from (Teo, et al., 2003)

- 我們組織正考慮採用 ISO 27001
- 我們組織在未來相當有可能採用 ISO 27001

Current status of organization’s ISMS

- 目前**無採用資訊安全管理認證之計畫**、也尚未評估是否採用。
- 目前**正在評估是否採用資訊安全管理認證**，但尚未確定採行何種資訊安全管理之建置
- 已確定採用**非 ISO 27001** 之資訊安全管理系統。(例如已採行 CNS 27001、COBIT、ITIL 或其他已包含資訊安全相關內容的認證或系統之建置)
- **已確定採用 ISO 27001 認證**，但尚未開始建置工作，預計西元_________年月開始建置工作，預計將在西元_________年____月通過認證。(或已有計畫建置但不認證)
- **已確定採用 ISO 27001 認證**，目前正在建置當中，預計將在西元_______年____月通過認證。(或正在建置但不認證)
- 已經在西元_________年____月**通過 ISO 27001 認證**，並正式上線運作中。
- 曾經在西元_________年____月通過認證，但目前**不持續維護**。

Organization size (capital)

- 無資本額(如學校、政府機關)、1 千萬以下、1 千萬至 3 千萬、3 千萬至 5 千萬、5 千萬至 1 億、1 億至 5 億、5 億至 20 億、20 億至 50 億、50 億至 100 億、100 億以上

Organization size (number of employees)

- 100 人以下、101 人至 200 人、201 至 500 人、501 至 1000 人、1001 至 2000 人、2001 至 5000 人、5001 至 10000 人、10001 以上

IT department size (number of employees in IT department)

- 15 人以下、16 至 30 人、31 至 60 人、61 至 100 人、101 至 200 人、201 至 300 人、301 至 500 人、500 人以上

Overall IT budget

- 1 百萬以下、1 百萬至 5 百萬、5 百至 1 千萬、1 千至 3 千萬、3 千至 5 千萬、5 千萬至 1 億、1 億至 3 億、3 億至 5 億、5 億至 10 億、10 億以上

Security budget (percentage in overall IT budget)

- 0~3%、4~6%、7~9%、10~15%、15%以上

Industry

- 政府機關、學校機關、科技及製造業(含資通、軟體等）、服務業、醫療機構、金融業(含銀行、證券、保險）、財團法人、其他