# 以多重理論建構資訊安全委外廠商評選量表

張俊陽
國立高雄應用科技大學
資訊管理系 副教授
cyc@cc.kuas.edu.tw

葉如慧
國立高雄應用科技大學
資訊管理系 碩士生
1093345111@cc.kuas.edu.tw

郭嘉偉
國立高雄應用科技大學
資訊管理系 碩士生
1095345110@cc.kuas.edu.tw

## 摘要

近年來資訊安全委外成為資訊安全管理的重要議題，而委外時最重要的關鍵即在於如何選擇承包商。因此，本研究目的在於建構資訊安全委外廠商評選量表。首先以委外供應商評選指標為基礎，而後加入代理理論與交易成本理論相關指標，並透過 ISO/IEC 27001:2005 與 CIA 原則修正原始指標以提出資訊安全委外廠商評選準則，最後由專家審查該準則並設計問卷。問卷結果經由分析後本研究提出 5 個構共 55 個評選資訊安全委外廠商之指標，以供學術與實務上之參考。

**關鍵詞**：資訊安全委外、評估指標、代理理論、交易成本理論。

## Abstract

Information security outsourcing has been one of the important issues facing information security management recently. One of the most critical steps in outsourcing is supplier selection. The aim of this study is to develop a reliable and valid information security outsourcing supplier selection criteria. The research process has the following important steps. First, we adopted Yang and Huang's outsourcing Supplier Selection indicators for criteria development. Second, applying Agency Theory and Transaction Cost Theory to strengthen the criteria then modified criteria by ISO/IEC 27001:2005 and CIA principles. At last, criteria examined by experts and we designed a questionnaire and used factor analysis to analyze data collected from Taiwanese firms. Our results provided five dimensions and fifty-five indicators. Implications for theory and practice are discussed.

**Keywords**: Information security outsourcing、Supplier Selection Criteria、Agency Theory、Transaction Cost Theory

## 1. 前言

在現代社會中，資訊科技已是企業日常營運中不可或缺的一環(Bermúdez et al., 2007)，但伴隨資訊科技日新月異而來的是更多安全上的挑戰(Mouratidis & Giorgini, 2007)。然而，不是每個企業都有足夠的空間與經費去聘請資訊安全專業人員。此時，企業為專注在核心能力上、提供更好的服務品質並降低成本，勢必考慮將非核心能力之相關問題委由專業人士處理(Marshall et al., 2007; Liston et al., 2007; Mojsilović, 2007)。

另一方面，資訊安全委外的概念，亦在近幾年逐漸受到注目，這是由於安全是相當極具專業的技術領域，大多數企業無法達到一定的專業水準來維護管理企業的安全問題，於是開始有企業致力於安全服務，以提供支援缺乏此專業能力的企業(Navarro, 2001; Karyda et al., 2006)。然而，由於資訊安全本身包含了機密性、完整性與可用性 (Schultz et al., 2001)，其牽涉了企業內部的商業機密，加上企業本身往往缺乏在資訊安全方面的專業人員(Navarro, 2001)，因此，企業在資訊安全方面能力明顯的不足。

根據上述學者觀點，可得知企業為抵禦來自於組織外部的資訊安全威脅、專注於發展核心能力、提供良好服務並降低成本將資訊安全委外成為未來必然的趨勢。

而委外最重要的就是如何選擇承包商(Wadhwa & Ravindran, 2007; Aissaoui et al., 2007)，選擇適合的承包商會提升委外成功的機率，而成功的委外可以帶來許多效益(Grover, 1996)。由此可知，企業如何根據內部資訊安全需求選擇適當之委外廠商便成為重要的議題。基於以上原因，本研究目的在於以過去委外與供應商評選指標為基礎推導出資訊安全委外廠商之評選指標。

## 2. 文獻探討

資訊安全委外的目的就是讓企業達到資訊安全與委外的目標，包含降低成本、提升績效、安全、專業技術、電腦應用、支援和財務分配(Axelrod, 2004)，故本研究在委外的部分將以評選委外及供應商之評估指標為基礎，再結合經常被用來探討委託人與承包商之間關係的代理理論與交易成本理論。資訊安全的部分則是透過 ISO/IEC27001:2005 內容、CIA 原則將指標修正，以建構本研究資訊安全委外廠商之評估指標。

### 2.1 資訊安全委外

由於過去對於資訊安全委外並無明確定義之文獻，因此，本小節將針對資訊安全及委外相關文獻做一整理及說明，進而對資訊安全委外定義。

#### 2.1.1 資訊安全

##### 2.1.1.1 定義

資訊安全是指保護資料不受到損害的程序(Misra et al., 2007)。而 Gollmann(1999)則定義資訊安全是指處理並且預防電腦系統使用者非法授權之行為，主要更是為了避免被未授權的使用者存取電腦內的資源(Sodiya et al., 2004)。因此，資訊安全是為了用來防止未授權的任何非法行為對資訊系統造成傷害的政策、程序，以及方法(Laudon et al., 2000)。另有多位學者認為資訊安全係指能保護系統中資料的機密性、完整性與可用性(Finne, 2000; Schultz, et al., 2001; Von Solms, 2005 & 2006; Yeh, et al., 2007)。資訊安全是一個存在組織內各部門的多面向問題(Gupta & Hammond, 2005)，每個人都應該重視。

因此，本研究認為資訊安全即指保護資料不受到損害，進而達到機密性、完整性與可用性目標的程序。

##### 2.1.1.2 資訊安全目標

資訊安全委外的目的就是希望可以藉由外部廠商的協助達到公司資訊安全的目標。

根據國際標準組織(International Organization for Standardization，ISO)2004 年所制定的 ISO/IEC 13335-1 提出的資訊安全目標(CIA 原則)如下：

1. 機密性(Confidentiality)：為資訊安全必須能確定唯有通過認證的使用者才得以存取資料。
2. 完整性(Integrity)：是指當資訊在經過保護及傳送的過程中，仍能的正確性及真確性。
3. 可用性(Availability)：即為通過認證的使用者隨時都可取得所需的資訊。

資訊安全委外最主要的目的就是達到組織資訊安全的目標，因此本研究將以 CIA 原則修正評選資訊安全委外廠商的指標。

##### 2.1.1.3 資訊安全系統規範

資訊安全委外廠商所提供的軟體應符合顧客對資訊安全的需求，然而，資訊安全包羅萬象，應如何判斷使用的資訊安全系統是否符合標準？

現有的資訊安全系統規範有 TCSEC(Trusted Computer System Evaluation Criteria) 、 COBIT(Control Objectives for Information and Related Technology)以及英國資訊安全管理標準訂定的 BS 7799 三種規範，其中以 BS 7799 最為完整，共分為三個部分。

第一、二部分並經過 ISO 認證目前最新版本分別稱為 ISO/IEC 27002:2005、ISO/IEC 27001:2005，ISO/IEC 27002:2005 只是一個實務上的準則而 ISO/IEC 27001:2005 則是一套完整的驗證規範。ISO/IEC 27001:2005 包含 11 個控制領域、 39 個控制目標、 133 個控制要點。其 11 個控制領域如下：

1. 安全政策。
2. 組織的資訊安全。
3. 資產管理。
4. 人員安全。
5. 實體及環境安全。
6. 通訊與操作管理。
7. 存取控制。
8. 資訊系統的取得、發展及維護。
9. 資訊安全事故管理。
10. 業務持續運作管理。
11. 遵循事項。

因 ISO/IEC 27001:2005 中的 133 個控制要點為組織資訊安全之指導原則而非目標，故本研究以 ISO/IEC 27001:2005 的 39 個控制目標與 CIA 原則相互配合來修正委外與供應商之評估準則。

### 2.1.2 委外

由於本研究建構評選資訊安全委外廠商之指標是由評選委外及供應商指標轉換而來，本小節將探討委外的定義及經常用來探討委託商及承包商之間的代理理論與交易成本理論相關文獻。

#### 2.1.2.1 定義

委外(Outsourcing)是”outside resource using”的縮寫，而outside是指從公司外部創造價值而非從公司內部(Yang et al., 2007)。過去文獻上關於委外的相關定義有：委外是指公司與第三方勞動者之間轉包契約的關係(Heshmati, 2003)，即是將企業內部非主流的活動轉移到一個外部的供應商(Benoit et al., 2004)；將組織中的資訊系統和相關服務的部分或全部轉交由第三者管理，以達到所需要的結果(Willcocks et al., 1995)；指企業將特定服務和系統的執行工作與管理委由第三者承擔(Alner & Marie, 2001)。

因此，本研究認為委外即將公司內部非核心能力之服務或系統委由外部公司承擔。

綜合上述文獻，本研究定義資訊安全委外為委託外部廠商協助、保護公司內部資訊不遭受非法侵害，而提供公司相關系統與服務之程序。

#### 2.1.2.2 相關理論

委外是涉及供應商與顧客雙方關係的議題，過去委外相關研究中代理理論與交易成本理論經常被拿來探討委託人與承包商之間的關係(Bahli & Rivard 2003; Zhengzhong et al., 2005)。 Moynihan(2002)運用代理理論來探討委外管理與策略之議題，而交易成本理論則作為委外研究中如何降低交易成本經常引用的理論(Gan, 2006)。

代理理論(Agency Theory)是1970年代經濟學者用來研究委託人與代理人之間風險分攤的問題(Michael & William, 1976)。後來有許多學者將其應用於探討人與人之間的代理關係(Ndubisi et al., 2005; Morgan et al., 2007)，而委外即是委託人將非核心能力的部分交由委外廠商代理。

而交易成本理論(Transaction Cost Theory)是指企業在決定內製或委外時交易成本提供了一個重要的指標(Steven, 2007)，而交易成本主要是因為委託人與代理人之間資訊不對稱所造成的(Zhang & Zhang, 2007)，如何降低交易成本是委外重要的議題(Yang &Huang, 2000；Chan & Chan, 2004; Kakouris et al., 2006)。

因此，本研究將代理理論與交易成本理論相關指標加入到指標當中。

### 2.2 評估指標

回顧過去資訊安全相關之研究並無評選資訊安全委外廠商指標可供參考，因此本研究透過蒐集委外與供應商評估指標之文獻結合委外經常使用的代理理論與交易成本理論，並透過ISO/IEC 27001:2005與CIA原則修正指標以建構評選資訊安全委外廠商之指標。資訊安全委外廠商評選量表推導流程如下圖所示：

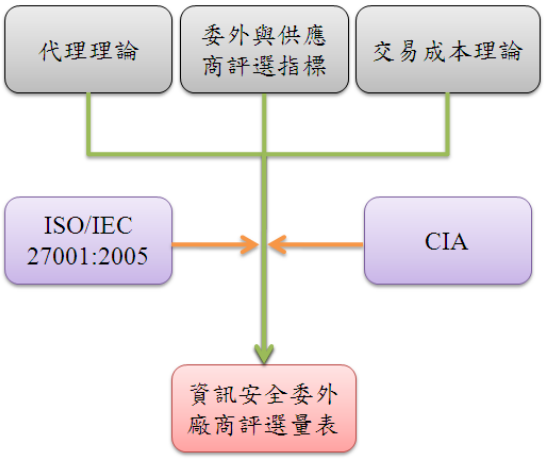


**圖 1 資訊安全委外廠商評選量表推導流程**

#### 2.2.1 委外及供應商評選之重要構面

在委外及供應商評選之相關研究中，本研究以Yang & Huang(2000)提出的管理、策略、技術、經濟、品質五個評選資訊系統委外廠商的構面為基礎，另外再輔以5篇委外及供應商評選構面之文獻，整理如下。

**表 1 委外及供應商之評選構面**

| 學者 | 評估構面 |
|---|---|
| Collins & Bechler(1999) | 技術能力、策略適配、能力需符合安全、健康和環境的標準、道德行為、成本、周轉能力、供應的安全性、顧客服務導向、致力於改善 |
| Yang & Huang(2000) | 管理、策略、技術、經濟、品質 |
| Chan & Chan(2004) | 成本、交貨期間、彈性、創新性、品質及服務 |

| 學者 | 評估構面 |
|---|---|
| Yang & Chen(2006) | 品質、經濟、顧客服務、生產力、IT 系統、設計及技術能力 |
| Kakouris et al.(2006) | 程序與設計能力、管理能力、財務、計劃與控制系統、與顧客間的關係 |
| Wang & Yang(2007) | 經濟、資源、策略、風險、管理、品質 |

資料來源：本研究整理

根據上述文獻，本研究歸納出選擇資訊安全委外廠商共 5 個評估構面：管理(Management)、策略(Strategy)、專業技術(Professional technical)、經濟(Economics)及服務品質(Service Quality)。

### 2.2.2 委外及供應商評選之重要指標

本小節將依據管理、策略、專業技術、經濟及服務品質 5 個構面蒐集委外及供應商評估指標及之文獻，整理於表 2。

**表 2　委外及供應商評估指標**

| | |
|---|---|
| 管理 | |
| • 刺激資訊部門改善績效<br>• 解決員工不足的問題<br>• 增進資訊部門管理的能力<br>• 增進資訊部門控制的能力 | Yang & Huang(2000) |
| • 委外廠商計劃的能力<br>• 委外廠商控制的能力 | Kakouris et al. (2006) |
| 策略 | |
| • 供應商的商譽 | Ellram(1990) |
| • 供應商的公司地點<br>• 供應商的市場佔有率 | Akomode, et al.,(1998) |
| • 專注於核心競爭能力<br>• 與委外廠商建立策略聯盟，能補足缺乏的資源或技術<br>• 透過策略聯盟將核心能力串聯起來，組織新公司開發新產品並銷售<br>• 風險分擔 | Yang & Huang(2000) |
| 專業技術 | |
| • 供應商的產業知識 | Jones(1994) |
| • 供應商軟體技術能力<br>• 供應商硬體技術能力 | Akomode.O. J. et al.(1998)： |
| • 從委外廠商學習新的軟體技術<br>• 從委外廠商獲得新技術 | Yang & Huang(2000) |
| • 擁有的技術可以保持最大的獨立性<br>• 擁有的技術可以保持最大的靈活性<br>• 為求改善不斷尋求支援 | Forster (2003) |
| • 委外廠商過去的經驗 | Kakouris et al.( 2006) |
| • 能對非預料中的事件和突發狀況做出回應 | Menon et al.(1998) |
| 經濟 | |
| • 供應商的價格 | Dickson,G.W (1966) |
| • 供應商財務的穩定性 | Ellram(1990) |
| • 將固定成本轉換為變動成本<br>• 增進財務的靈活性 | Yang& Huang(2000) |
| • 透過和廠商的合作增進資產的利用<br>• 減少資源的重複及浪費 | Kakouris et al.( 2006) |
| 服務品質 | |
| • 有現代化設備<br>• 有具吸引力的服務設施<br>• 服務人員整潔的儀表<br>• 公司服務與設施相配合<br>• 對顧客的承諾都能及時完成<br>• 關心並協助顧客解決問題<br>• 公司是可靠的，能第一次就提供完善服務<br>• 於承諾時間內，提供適當服務<br>• 正確紀錄，保存顧客資料<br>• 需通知顧客服務時間<br>• 顧客能得到適當快速的服務<br>• 服務人員樂意協助與服務顧客<br>• 服務人員能立即提供服務<br>• 服務人員是值得信任的<br>• 顧客在服務人員互動中感到安全<br>• 服務人員很有禮貌<br>• 服務人員可得到公司適當支持，以提供更好的服務<br>• 公司能針對不同顧客提供個別服務<br>• 服務人員能給予顧客個別關懷<br>• 服務人員能瞭解顧客的個別需要<br>• 公司能以顧客權益為優先考量<br>• 公司的服務時間能符合顧客需要 | Parasuraman et al.(1988) |

資料來源：本研究整理

### 2.2.3 代理理論指標

代理理論的本質在於探討代理的風險與

代理所產生的成本。因此，本研究在策略及經濟構面加入了代理理論相關評估指標。

**表 3　代理理論評估指標**

| 策略 | |
|---|---|
| • 委託人與代理人想達到的目標是否不一致<br>• 委託人與代理人對風險的處理態度不一致將會提高所分擔的風險 | Ndubisi et al. (2005) |
| • 委託人對代理人的監控可以預防代理人投機 | Morgan et al.(2007) |
| 經濟 | |
| • 在委託人與代理人之間監控能有效降低資訊不對稱進而降低成本 | Morgan et al.(2007) |

### 2.2.4 交易成本理論指標

交易成本理論在於探討交易的過程中因環境不確定性、資訊不對稱等原因所造成的成本，因此，本研究在經濟構面加入交易成本理論指標予以探討。

**表 4　交易成本理論評估指標**

| 經濟 | |
|---|---|
| • 降低資訊系統開發的成本<br>• 降低資訊系統維護的成本 | Yang &Huang (2000) |
| • 委外廠商能有效降低因環境不確性所帶來的交易成本 | Benoit et al.(2004) |

惟上述指標並非針對資訊安全委外廠商，故本研究藉由 ISO/IEC 27001:2005 及 CIA 原則將指標修正為適合評選資訊安全委外廠商之指標。

## 3. 研究方法

本研究經由文獻探討彙整過去學者關於委外與供應商之評選指標後，結合代理理論與交易成本理論，然後以 ISO/IEC27001:2005 與 CIA 原則修正指標以建構本研究所需之評選量表，並透過問卷向目前業界相關人員蒐集樣本資料。根據所得資料進行探索性因素分析，瞭解變數是否為衡量資訊安全委外廠商之指標，並根據 Chen and Li(2007)的建議，在發展量表時，做完探索性因素分析後應再以驗證性因素分析檢驗量表的建構效度。研究方法如下圖所示：


**圖 2 研究方法流程圖**

### 3.1 問卷設計

本研究問卷資料蒐集分為兩個階段，第一階段為問卷之預試，目的在於修正問卷可能存在的缺點與不良問項，第二階段即為問卷的正式調查。

問卷透過文獻探討歸納出評選資訊安全委外廠的 5 個構面與 58 個指標，將其轉換為本研究之問卷。問卷採用李克特五點量表尺度(Likert Scale)來衡量，受測者於「非常重要」、「重要」、「普通」、「不重要」、「非常不重要」五個選項中勾選一項。問卷完成後，即邀請 3 位專家學者進行前測工作，聽取專家學者的意見後進行問項內容之修正（內容如附錄 A）。

### 3.2 研究樣本

本研究之受訪對象為上班族，且因 Gupta & Hammond(2005)提出資訊安全是存在於公司各部門中的問題，故受訪對象不受限於資訊部門。

### 3.3 資料分析方法與工具

本研究以 SPSS 12.0 for Windows 與 Lisrel 8.51 作為資料分析與檢驗的工具，運用之資料分析方法包括敘述統計、探索性因素分析、驗證性因素分析，各分析方法詳細如下：

(1) 敘述統計(Descriptive Statistic)

敘述統計主要應用在問卷對象之基本資料分析，目的是為了解回收樣本之一般性數據

資料及其分布狀況，並針對回收問卷的各項特性進行分析。

(2) 項目分析

屬於李克特性質的量表才能進行項目分析與信度分析。本研究採用項目分析極端組檢核法（又稱為內部一致性效標法）為檢驗預試量表中每一個題項是否具有鑑別度，改善量表的品質使正式調查之問卷更趨完善。

(3) 信度分析

所謂信度(reliability)，係指衡量工具之可靠性，亦即重覆進行調查或測量，其所得結果一致的程度。一般來說，在統計分析上之問卷信度測量是以 Cronbach's α 係數進行檢定。係收越趨近於 1 信度越高，代表量表之穩定性越高。

(4) 探索性因素分析 (Exploratory Factor Analysis)

根據國外學者 Kim & Mueller(1978)的研究，因素分析發展的最初目的，是在簡化一群龐雜的測量，藉此找出可能存在於觀察變項後的因素結構，使之更為明確，增加理解度。本研究之因素分析是採用主成分分析法(principal component analysis)來萃取相關因素。其因素的選取，如根據陡坡圖(scree plot)，似較不易選取適當的因素數目，故本研究再依據 H. F. Kaiser (1958)的選取準則，將特徵值(eigenvalue)大於 1 的因素，選取為因素個數。為使共同因素的解釋與命名更為方便，必須旋轉因素軸，以使各個因素的意義可以顯得比較清晰明顯。而轉軸(rotation)可以使得因素負荷量易於解釋，常用的轉軸法有，最大變異法(varimax)與四次方最大值法(quartimax)等。

本研究採用最大變異法，其優點在於因素間所提供的資訊不會重疊，因此在轉軸後，可以使變項在每個因素的負荷量不是變大就是變得更小，讓因素的解釋更為清楚明瞭。因此，本研究採用主成份分析法與最大變異法進行轉軸。

(5) 驗證性因素分析 (Confirmatory Factor Analysis)

當研究者得知量表或問卷是由數個潛在構面或因素所構成，為了確認量表所包含的因素是不與最初探究的構念相同而加以檢驗，此時量表的各因素與其題項均已固定，研究者所要探究的是量表的因素結構模式是否與實際蒐集的資料契合，指標變項是否可以有效作為因素構念的測量變項，此種因素分析的程序，即稱為驗證性因素分析。(吳明隆, 2006)

本研究目的在於建構資訊安全委外廠商評選量表，根據上述驗證性因素分析的定義及 Mei-Ling and Chia-Chin(2007)建議在發展量表時，做完探索性因素分析後應再以驗證性因素分析檢驗量表的建構效度，因此本研究在做完探索性因素分析後，將以驗證性因素分析加以檢驗資訊安全委外廠商評選量表之建構效度。

## 4. 實證結果與分析

本研究依據研究目的，採用 SPSS12.0 與 Lisrel 8.51 進行問卷資料分析與檢驗，以建構資訊安全委外廠商評選量表。

### 4.1 預試結果分析

#### 4.1.1 樣本資料敘述統計分析

本研究係以國內公民營企業組織為量表預試對象。於 2007 年 12 月間發出問卷 150 份，扣除無效問卷，共回收有效問卷 128 份，有效回收率為 85 %。經由 SPSS 12.0 的分析結果可以發現填答者的公司產業類別以資訊服務業最多，約佔 33%。公司的員工總數則以 200 人以上佔最多，約佔 50%。公司資訊部門人數則是 10-29 人佔最多，31%。

#### 4.1.2 項目分析

本研究採用項目分析中的極端組檢核法測驗題目的鑑別度。將預試的資料依據效標，將受測者的得分依照高低順序排列，然後選出最高分（前 25%）與最低分（後 25%）的兩群人，稱為效標組（高分組與低分組）。然後將兩個組別進行獨立樣本 T 檢定，結果顯示有 3 個問項（資訊安全委外廠商能刺激本公司資訊部門改善工作績效、資訊安全委外廠商能對於本公司資訊的機密性、完整性及可用性有著良好的控制能力、資訊安全委外廠商的市場佔有率比較高）未達顯著，故予刪除。

#### 4.1.3 信度分析

本研究採用信度分析主要的目的是在衡量量表內各問項之內部一致性程度。Cronbach's α 值，如表 5 所示，管理、專業技術、經濟與服務品質四個構面的 Cronbach's α 均大於 0.7，表示該四個構面問項的內部一致性均佳。策略面的 Cronbach's α 為 0.643 亦接近 0.7 故不刪除其中的問項來提升信度。

**表 5 各構面之信度分析**

| 構面 | Cronbach's α |
|---|---|
| 管理 | 0.713 |
| 策略 | 0.643 |
| 專業技術 | 0.843 |
| 經濟 | 0.864 |
| 服務品質 | 0.908 |

預試結果經由項目分析與信度分析本研究刪除 3 個不良問項，共 55 個題項進行問卷之正式調查。

### 4.2 正式調查結果分析

#### 4.2.1 決定樣本數

量表正式調查之樣本數參考 Hair et al.(1998)應為獨立變項的 5~10 倍，且以 LISREL 驗證結構時，樣本應介於 100~400 間，並考慮問卷回收率及無效問卷之問題後，本研究擬發出 400 份正式調查問卷。

#### 4.2.2 樣本結果分析

待分析。

## 5 結果與討論

### 5.1 預期貢獻

本研究之貢獻可分為學術與實務兩方面。在學術方面過去沒有評選資訊安全委外廠商指標相關研究，本研究經由文獻探討彙整委外與供應商評選指標，結合代理理論與交易成本理論指標，最近再以 ISO/IEC 27001:2005 與 CIA 原則將指標修正，為後續想要研究資訊安全委外相關議題，提供了評估指標。在實務方面，對企業而言，提供給企業管理者資訊安全委外時一個評量參考；對承包商而言，業者可以藉此量表作為公司日後營運策略調整的參考。

## 參考文獻


**1. 中文部分**

[1] 吳明隆， ***結構方程模式 - SIMPLIS 的應用***，五南圖書出版，2006。

**2. 英文部分**

[1] Aissaoui, N., Haouari, M. and Hassini, E., "Supplier selection and order lot sizing modeling: A review," ***Computers & Operations Research***, Vol. 34, Issue 12, pp. 3516-3540, 2007.

[2] Akomode, O. J., Lees, B. and Irgens C., "Constructing customised models and providing information to support IT outsourcing decisions," ***Logistics Information Management***, Vol. 11, No. 2, pp. 114-127, 1998.

[3] Alner and Marie, "The Effects of Outsourcing on Information Security", ***Information Systems Security***, Vol. 10, Issue 2, pp. 35-43, 2001.

[4] Axelrod, C. W., ***Outsourcing Information Security***, Artech House Publishers, 2004.

[5] Bahli B. and Rivard S., "The information technology outsourcing risk: a transaction cost and agency theory-based perspective," ***Journal of Information Technology***, Vol. 18 Issue 3, pp. 211-221, 2003.

[6] Benoit, A. A., Rivard, S., Patry, M., "A transaction cost model of IT outsourcing," ***Information & Management***, Vol. 41, pp. 921–932, 2004.

[7] Bermúdez, J., Goñi, A., Illarramendi, A. and Bagüés, M. I., "Interoperation among agent-based information systems through a communication acts ontology," ***Information Systems***, Vol. 32, Issue 8, pp. 1121-1144, 2007.

[8] Chan, F. T. S. and Chan, H. K., "Development of the supplier selection model – a case study in the advanced technology industry," ***Proceedings of the Institution of Mechanical Engineers***, Vol. 218, No. 12, pp. 1807-1824, 2004.

[9] Chen, M. L. and Li, C. C., "Cancer Symptom Clusters: A Validation Study," ***Journal of Pain and Symptom Management***, Vol. 34, Issue 6, pp. 590-599, 2007.

[10] Collins, R. and Bechler, K., "Outsourcing in the Chemical and Automotive Industries: Choice or Competitive Imperative?" ***The Journal of Supply Chain Management***, Vol.35, No.4, pp.4-11, 1999.

[11] Dickson, G.W., "An analysis of vendor selection systems and decisions," ***Journal of Purchasing***, Vol. 2, No. 1, pp. 28-41,1966.

[12] Ellram, L. M., "The Supplier Selection Decision in Strategic Partnerships,"

***International Journal of Purchasing and Materials Management***, Vol. 26, Issue 4; pp. 8-14 , 1990.

[13] Finne, T., "Information systems risk management: Key concepts and business processes," ***Computers & Security***, Vol. 19, No. 3, pp. 234-242, 2000.

[14] Foster, T.A., "Engineering the 3PL selection process," ***Logistics Management***, Vol. 42 No. 6, pp. 3-11, 2003.

[15] Gan, W., "Analysis on the Costs of IT-Outsourcing," ***Service Operations and Logistics, and Informatics***, pp. 785-789, 2006.

[16] Gollmann, D., ***Computer Security***, John Wiley and Sons Ltd, 1999.

[17] Grover, V., Cheon, M. J. and Teng, J. T. C. , "The effect of service quality and partnership on the outsourcing of information systems functions," ***Journal of Management Information Systems***, Vol. 12, No.4, pp.89-116, 1996.

[18] Gupta, A. and Hammond, R.,"Information systems security issues and decisions for small businesses An empirical examination," ***Information anagement & Computer Security***, Vol. 13 No. 4, pp. 297-310, 2005.

[19] Hair, J. F., Anderson, R. E., Tatham, R. L., and Black, W. C., ***Multivariate data analysis***, 5th ed. N. J : Prentice Hall, 1998.

[20] Heshmati, A., "Productivity Growth, Efficiency and Outsourcing in Manufacturing and Service Industries," ***Journal of Economic Surveys***, Vol. 17, No.1, pp. 80-112, 2003.

[21] Jones, C. ,"Evaluating software outsourcing options," ***Information Systems Management***, Vol. 11, Issue 4, pp. 28-33, 1994.

[22] Kaiser, H. F., "The varimax criterion for analytic rotation in factor analysis," ***Psychometrika***, Vol. 23, pp. 187-200, 1958.

[23] Kakouris, A. P., Polychronopoulos, G., Binioris, S., "Outsourcing decisions and the purchasing process : a system-oriented approach," ***Marketing Intelligence & Planning***, Vol. 24, Iss. 7; pp. 708-729, 2006.

[24] Karyda, M., Mitrou, E., and Quirchmayr, G. , "A framework for outsourcing IS/IT security services," ***Information Management & Computer Security***, Vol.14, No.5, pp.402-415, 2006.

[25] Laudon, K. C., and Laudon, J, P., ***Management information systems: organization and technology in the networked enterprise***, Upper Saddle River, NJ: Prentice Hall, 2000.

[26] Kim and Mueller, ***Factor analysis: Statistical methods and practical issues***, Sage Publications, 1978.

[27] Liston, P., Byrne, P. J. and Heavey, C., "An evaluation of simulation to support contract costing," ***Computers & Operations Research***, Vol. 34, Issue 12, pp. 3652-3665 , 2007.

[28] Marshall, D., McIvor, R. and Lamming, R., "Influences and outcomes of outsourcing: Insights from the telecommunications industry," ***Journal of Purchasing and Supply Management***, In Press, Corrected Proof, Available online 1, 2007.

[29] Menon, M.K., McGinnis, M.A. and Ackerman, K.B., "Selection criteria for providers of third-party logistics services: an exploratory study," ***Journal of Business Logistics***, Vol. 19, No. 1,pp. 121-137,1998.

[30] Michael C. J. & William H. M., "Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure," ***Journal of Financial Economics***, Vol. 3,pp. 305-360, 1976.

[31] Misra, S. C., Kumar, V. and Kumar U., "A strategic modeling technique for information security risk assessment," ***Information Management & Computer Security***, Vol. 15, No. 1, pp. 64-77, 2007.

[32] Mojsilović, A., Ray, B., Lawrence. R. and Takriti, S., "A logistic regression framework for information technology outsourcing lifecycle management," ***Computers & Operations Research***, Vol. 34, Issue 12, pp. 3609-3627, 2007.

[33] Morgan, N. A., Kaleka, A. and Gooner, R. A., "Focal supplier opportunism in supermarket retailer category management," ***Journal of Operations Management***, Vol. 25, Issue 2, pp. 512-527, 2007.

[34] Mouratidis, H. and Giorgini, P., "Security Attack Testing (SAT)—testing the security of information systems at design time," ***Information Systems***, Vol. 32, Issue 8, pp. 1166-1183, 2007.

[35] Moynihan, T., "Coping with client-based 'people-problems' : the theories-of-action of experienced IS/software project managers," ***Information & Management***, Vol. 39, pp. 377–390, 2002.

[36] Navarro, L., "Information Security Risks and Managed Security Service, " ***Information Security Technical Report***, Vol. 6, No.3, pp.28-36, 2001.

[37] Ndubisi, N. O., Jantan, M., Hing, L. C. and Ayub, M. S., "Supplier selection and management strategies and manufacturing flexibility," ***The Journal of Enterprise Information Management***, Vol. 18 No. 3, pp. 330-349, 2005.

[38] Parasuraman, A., Berry, L.L. and V.A. Zeithaml, "SERVQUAL : A Multiple-Item Scale for Measuring Consumer Perception of Service Quality," ***Journal of Marketing***, Vol. 64, No. 1, pp. 12-40, 1988.

[39] Schultz, E. E., Proctor, R. W., Lien, M. C. and Salvendy, G., "Usability and Security An Appraisal of Usability Issues in Information Security Methods," ***Computers & Security***, Vol. 20, No. 7, pp. 620-634, 2001.

[40] Sodiya, A. S., Longe, H. O. D., and Akinwale, A. T., "A new two-tiered strategy to intrusion detection," ***Information Management & Computer Security***, Vol. 12, No. 1, pp. 27-44, 2004.

[41] Steven, C. M., "Transaction cost entrepreneurship," ***Journal of Business Venturing***, Vol. 22, Issue 3, pp. 412-426, 2007.

[42] Von Solms, B., "Information security - The fourth wave," ***Computers & Security***, Vol. 25, No. 3, pp. 165-168, 2006.

[43] Von Solms, S.H., "Information Security Governance – Compliance management vs operational management," ***Computers & Security***, Vol. 24, No. 6, pp. 443-447, 2005.

[44] Wadhwa, V. and Ravindran, A. R.,"Vendor selection in outsourcing," ***Computers & Operations Research***, Vol. 34, Issue 12, pp. 3725-3737, 2007.

[45] Wang, J. J., Yang, D. L., "Using a hybrid multi-criteria decision aid method for information systems outsourcing," ***Computers & Operations Research***, Vol. 34, pp. 3691-3700, 2007.

[46] Willcocks, L., M. Lacity and G. Fitzgerald, "Information Technology Outsourcing in Europe and the USA: Assessment issues", ***International Journal of Information Management***, Vol. 15, No. 5, pp. 333-351, 1995.

[47] Yang, C. and Huang, J. B., "Adecision model for IS outsourcing," ***International Journal of Information Management***, Vol. 20, pp. 225-239, 2000.

[48] Yang, C. C. and Chen, B. S., "Supplier selection using combined analytical hierarchy process and grey relational analysis," ***Journal of Manufacturing Technology Management***, Vol. 17, No. 7, pp. 926-941, 2006.

[49] Yang, D. H., Kim, S., Nam, C., Min, J. W., "Developing a decision model for business process outsourcing", ***Computers & Operations Research***, Vol.34 , pp. 3769 – 3778, 2007.

[50] Yeh, Q. J. & Chang, J. T., "Threats and countermeasures for information system security: A cross-industry study," ***Information & Management***, Vol. 44, No. 5, pp. 4880-491, 2007.

[51] Zhang, J. L. and Zhang, F. R., "Mutual monitoring in a tradable water rights system: A case study of Zhangye City in Northwest China," ***Agricultural Water Management***, In Press, Corrected Proof, 2007.

[52] Zhengzhong S., Kunnathur, A.S. and Ragu-Nathan, T.S., "IS outsourcing management competence dimensions: instrument development and relationship exploration," ***Information & Management***, Vol. 42, Issue 6, pp. 901-919, 2005.

## 附錄 A

各位受訪者，您好：

本研究為發展評選資訊安全委外廠商之指標，先前已根據相關文獻彙整如下問卷。

問卷內容主要針對評選資訊安全委外廠商指標進行重要性分析調查，請您就專業上的考量，在下列各考核指標因素中，從「非常重要」至「非常不重要」分別給予評分，並請每題均答。

在此致上萬分感謝！本調查期能對公司未來在選擇資訊安全委外廠商時，有所參考與助益。您所填寫的結果僅供整體統計分析之用，絕不對外單獨發表，敬請安心作答。您的意見對本研究的成敗影響甚鉅，因此期望您撥冗填答。您熱心的協助，是本研究成功與否的關鍵，謹致十二萬分的謝意！

最後，感謝您的參與及配合，祝您：

居家平安　事事順心

國立高雄應用科技大學
資訊管理研究所
指導教授：張俊陽　博士
研 究 生：葉如慧　　敬上

1. 請問您所屬公司之產業別為何？

   □資訊服務業 □通訊業 □製造業 □批發業 □運輸業 □貿易業 □金融業 □不動產業 □其他

2. 貴公司員工總數約為：

   □ 20 人以下 □ 21-50 人 □ 51-100 人 □ 101-150 人 □ 151-200 人 □ 200 人以上

3. 貴公司資訊部門人數約為：

   □ 5 人以下 □ 6-9 人 □ 10-29 人 □ 30-49 人 □ 50 人以上

4. 您在公司中所屬單位為：

   □資訊部門 □人事部門 □會計部門 □其他

本研究定義所謂的「資訊安全委外」為委託外部廠商協助、保護公司內部資訊不遭受非法侵害，而提供公司相關系統與服務之程序。

以下問題請您假設貴公司將內部資訊安全之系統與服務委由外部公司負責時，應考慮的項目及所會帶來的影響分別給予評等。另外，問卷中所提到的機密性、完整性與可用性為 ISO 所定訂之資訊安全目標，其定義說明如下：

1. 機密性（Confidentiality）：機密性為資訊安全必須能確定唯有通過認證的使用者才得以存取資料，當不論任何人都可以輕易得知『機密』或『極機密』等級文件內容，這就形同沒有資訊安全。
2. 完整性（Integrity）：完整性是指當資訊在經過保護及傳送的過程中，仍能的正確性及真確性。現今所指的資訊完整性，大多是發生在網際網路的傳輸品質以及加解密技術上。
3. 可用性（Availability）：可用性即為通過認證的使用者隨時都可取得所需的資訊，除了保護系統的安全外，更應考慮到讓使用者隨時都可使用的便利性，確保被授權的使用者在需要存取資料時，可以順利獲得。

【請您針對下列各項指標做為評選資訊安全委外廠商時“管理”面之重要性給予評等打"✓"】

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| M1 | 資訊安全委外廠商能刺激本公司資訊部門改善工作績效 | ☐ | ☐ | ☐ | ☐ | ☐ |
| M2 | 資訊安全委外廠商能解決本公司資訊部門資訊安全人員不足的問題 | ☐ | ☐ | ☐ | ☐ | ☐ |
| M3 | 資訊安全委外廠商能增進本公司資訊部門管理的能力 | ☐ | ☐ | ☐ | ☐ | ☐ |
| M4 | 資訊安全委外廠商能增進本公司資訊部門控制的能力 | ☐ | ☐ | ☐ | ☐ | ☐ |
| M5 | 資訊安全委外廠商能對於本公司資訊的機密性、完整性及可用性有著良好的計劃能力 | ☐ | ☐ | ☐ | ☐ | ☐ |
| M6 | 資訊安全委外廠商能對於本公司資訊的機密性、完整性及可用性有著良好的控制能力 | ☐ | ☐ | ☐ | ☐ | ☐ |

【請您針對下列各項指標做為評選資訊安全委外廠商時“策略”面之重要性給予評等打"✓"】

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| S1 | 資訊安全委外廠商有著良好的商譽 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S2 | 資訊安全委外廠商的公司地點離本公司比較近 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S3 | 資訊安全委外廠商的市場佔有率比較高 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S4 | 資訊安全委外廠商能使本公司專注於核心競爭能力的發展 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S5 | 與委外廠商建立策略聯盟，能補足缺乏的資源或技術 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S6 | 與資訊安全委外廠商透過策略聯盟將核心能力串聯起來，組織新公司開發新產品並銷售 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S7 | 資訊安全委外廠商與本公司能分擔資訊安全事件發生的風險 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S8 | 資訊安全委外廠商與本公司想達到的資訊安全目標是一致的 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S9 | 資訊安全委外廠商與本公司對資訊安全風險的處理態度不一致將會提高所分擔的風險 | ☐ | ☐ | ☐ | ☐ | ☐ |
| S10 | 若資訊安全委外廠商允許本公司對其監控將可以預防資訊安全委外廠商投機 | ☐ | ☐ | ☐ | ☐ | ☐ |

【請您針對下列各項指標做為評選資訊安全委外廠商時“專業技術”面之重要性給予評等打"✓"】

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| T1 | 資訊安全委外廠商的資訊安全專業知識能協助本公司的資訊達到機密性、完整性與可用性 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T2 | 資訊安全委外廠商的軟體技術能力能協助本公司的資訊達到機密性、完整性與可用性 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T3 | 資訊安全委外廠商的硬體技術能力能協助本公司的資訊達到機密性、完整性與可用性 | ☐ | ☐ | ☐ | ☐ | ☐ |

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| T4 | 本公司能從資訊安全委外廠商學習新的軟體，以降低本公司發生資訊安全事件的風險 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T5 | 本公司能從資訊安全委外廠商獲得新的技術，以降低本公司發生資訊安全事件的風險 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T6 | 資訊安全委外廠商擁有的技術可以保持最大的獨立性 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T7 | 資訊安全委外廠商擁有的技術可以保持最大的靈活性 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T8 | 資訊安全委外廠商為求改善不斷尋求支援 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T9 | 資訊安全委外廠商過去擁有豐富的資訊安全事件經驗 | ☐ | ☐ | ☐ | ☐ | ☐ |
| T10 | 資訊安全委外廠商能對非預料中的資訊安全事件和突發狀況做出即時回應 | ☐ | ☐ | ☐ | ☐ | ☐ |

【請您針對下列各項指標做為評選資訊安全委外廠商時“經濟”面之重要性給予評等打”✓”】

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| E1 | 資訊安全委外廠商提供的價格較同業合理 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E2 | 資訊安全委外廠商財務的穩定性 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E3 | 資訊安全委外廠商能使本公司將資訊安全部分的固定成本轉換為變動成本 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E4 | 資訊安全委外廠商能增進本公司財務上的靈活性 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E5 | 透過和資訊安全委外廠商的合作能增進本公司資產的利用 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E6 | 資訊安全委外廠商能使本公司減少資源的重複及浪費 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E7 | 本公司對資訊安全委外廠商的監控能有效降低資訊不對稱進而降低成本 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E8 | 資訊安全委外廠商能降低本公司資訊安全管理系統開發的成本 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E9 | 資訊安全委外廠商能降低本公司資訊安全管理系統維護的成本 | ☐ | ☐ | ☐ | ☐ | ☐ |
| E10 | 資訊安全委外廠商能有效降低因環境不確性所帶來的交易成本 | ☐ | ☐ | ☐ | ☐ | ☐ |

【請您針對下列各項指標做為評選資訊安全委外廠商時“服務品質”面之重要性給予評等打”✓”】

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| Q1 | 資訊安全委外廠商有現代化的設備，能抵抗危害硬體設備之環境條件（如：火、水災） | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q2 | 資訊安全委外廠商有具吸引力的服務設施 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q3 | 資訊安全委外廠商服務人員整潔的儀表 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q4 | 資訊安全委外廠商服務與設施相配合 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q5 | 資訊安全委外廠商對顧客的承諾都能及時完成 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q6 | 資訊安全委外廠商關心並協助顧客解決問題 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q7 | 資訊安全委外廠商是可靠的，能第一次就提供完善服務 | ☐ | ☐ | ☐ | ☐ | ☐ |

| 題項 | 題目 | 非常重要 | 重要 | 普通 | 不重要 | 非常不重要 |
|---|---|---|---|---|---|---|
| Q8 | 資訊安全委外廠商於承諾時間內，提供適當服務 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q9 | 資訊安全委外廠商正確紀錄，保存顧客資料 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q10 | 資訊安全委外廠商需通知顧客服務時間 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q11 | 資訊安全委外廠商的顧客能得到適當快速的服務 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q12 | 資訊安全委外廠商服務人員樂意協助與服務顧客 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q13 | 資訊安全委外廠商服務人員能立即提供服務 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q14 | 資訊安全委外廠商服務人員是值得信任的 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q15 | 資訊安全委外廠商顧客在服務人員互動中感到安全 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q16 | 資訊安全委外廠商服務人員很有禮貌 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q17 | 資訊安全委外廠商服務人員可得到公司適當支持，以提供更好的服務 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q18 | 資訊安全委外廠商能針對不同顧客提供個別服務 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q19 | 資訊安全委外廠商服務人員能給予顧客個別關懷 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q20 | 資訊安全委外廠商服務人員能瞭解顧客的個別需要 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q21 | 資訊安全委外廠商能以顧客權益為優先考量 | ☐ | ☐ | ☐ | ☐ | ☐ |
| Q22 | 資訊安全委外廠商的服務時間能符合顧客需要 | ☐ | ☐ | ☐ | ☐ | ☐ |