# 建構醫院資訊安全風險管理架構與風險衡量之研究

張啓昌[1*] 孫培然[2] 陳進典[3]

## 摘 要

本研究目的為建構醫院資訊安全風險管理架構，藉以提供醫院組織人員對資訊安全認知的警覺輔助並達成風險有效衡量。研究模式建構係以ISO17799資訊安全標準為實務規劃，並結合修正期望效用理論與Riskit模式為理論基礎；進一步為驗證模式的可行性，本研究以中部某醫學中心推動資訊安全風險計畫為對象進行實地調查。結果顯示，本研究所得與先前學者的探討趨於一致，意即印證人類在面臨風險環境下其決策態度與行為並非是一致的，並且對於風險衡量方面的基數方法咸認為比Riskit模式所使用序數排列更為精確與可靠；本研究所發展的修正模式可以藉由冤參數兩階段的偏好選擇，確實且全面地反映出利害關係人的風險態度與決策行為。綜觀醫院資訊安全風險管理的經驗顯示，若能深入調查個別利害關係人對於風險認知的態度，就可以掌握不同階段潛在的風險因素，再利用冤參數方法據以衡量潛在的風險事件，即使有非預期危害事件發生亦可以將風險損失加以轉移與控制，進而達成風險管理的目標。由於本研究架構所探討利害關係人的決策態度與行為特性具有一般性的應用價值，可以提供其他資訊安全風險管理領域應用之參考。

關鍵詞：醫院資訊風險管理、修正期望效用理論、ISO17799、Riskit模式、冤參數方法

[1] 中山醫學大學 應用資訊科學學系暨碩士班
[2] 中山醫學大學附設醫院 資訊室
[3] 中山醫學大學 醫學系
* 通訊作者：張啓昌
通訊地址：40201台中市南區建國北路一段110號
聯絡電話：04-24730022 分機17107
電子信箱：threec@csmu.edu.tw

## 前　言

隨著社會環境的變遷、全民健保的實施以及醫療院所彼此的競爭，醫院因面臨前所未有的經營衝擊與挑戰，相繼導入資訊科技以期待有效提升經營績效與競爭優勢。由於醫院主要的職責在於提供病患良好的照護，一旦資訊系統遭受攻擊而無法正常運作，勢必會直接影響醫療照護的服務品質，間接亦可能造成病患流失等問題[1,2]。根據Mizani and Baykal認爲醫療院所資訊安全的保護範圍應避免造成：「人或財產的實體損害、隱私權侵犯、病歷資訊竄改或遺失以及操作完整性或一致性的危害」[3]。Paré指出：「積極的風險管理就是及早發現潛在問題與預防，以期減少訴訟與維持醫療機構的正常運作」[4]。相對於國內的研究文獻中[5]，亦明白指出醫療資訊安全與隱私議題的重要性，該研究並依據ISO/IEC 27001爲基礎進行檢核表的個案調查，但是面臨如何提升與衡量組織成員對於資訊安全認知的警覺性仍無所著墨。換言之，確保資訊安全不僅是單純的避免資訊被破壞、僞造或遺失等保護措施，若能強化組織成員對於資訊安全認知的警覺性，並藉由良善風險管理架構的設計與適當衡量機制的建立，是現階段醫院資訊安全風險重要的工作[5,6]。

現今各醫療院所的資訊化推動工作，推動成效看似良好，但根據國際經濟合作發展組織(OECD/PUMA)所做的調查顯示[7]，推動資訊科技(Information Technology, IT)計畫的成功率大約只有25%。雖然現階段醫院資訊安全風險管理的實務作法略有不同，但大部分都偏重在風險管理之辨認、分析與監控組織架構的建立，有關風險衡量的部分仍相當缺乏，而就風險管理的整體架構來說，風險衡量實爲風險管理流程中最爲關鍵的部分。再者，根據Kontio & Basili (1997)提出現存風險管理方法的障礙有[8]：1.風險管理技術認知很低；2.有許多理論及實務的限制；3.只有少數的方法能夠準確的定義風險；4.許多方法都不能在風險分析方面平衡利害關係人(stakeholder)的利益；5.無法提出實證說明這些風險管理的方法有用。換言之，風險衡量的成敗將會影響到風險管理的成敗，因爲風險不能準確地衡量將會很容易造成決策錯誤的情形發生，而錯誤的決策極可能會造成資訊系統失效，所以爲了要避免因風險衡量而造成決策上缺失，本研究覺得應該使用更爲客觀及準確的方法來進行風險衡量。

回顧現階段醫院資訊安全風險管理的文獻，多數僅止於探討資訊安全技術的進化與配置，仍無法對於資產、人員、面臨威脅及安全弱點所產生各種風險結果，提供一個明確量化指標與具體實務應用的方法。本研究爲解決上述問題將引用Kontio等人所發展Riskit風險模式爲理論基礎[8]，進一步改善該模式在風險衡量所使用序列效用損失函數(Ordinal Utility Loss Function)並非十分精確，且多年來受到許多學者質疑該序列效用理論是否能代表人類在風險下的決策行爲。根據風險衡量主觀性的議題在過去文獻的討論中：Ng在1984年曾經對von Neumannn和Morgenstern的期望效用理論做出了補

充，他認爲應以主觀機率爲加權來取代客觀機率。他認爲人們作決策時，是採用以心理上所感受到的機率，而導出所謂的「主觀期望效用」(Subjective Expected Utility，SEU)。進一步提出「S」形效用函數。認爲效用函數的曲線形狀會呈現波浪狀，即某一區間爲反凹的效用函數，另一區間爲反凸的效用函數，用以解釋爲何人類同時會有賭博及保險的兩種不同風險態度的決策行爲。而今，我們一般所謂的「期望效用理論」，若無特別說明，即是指奠基於von Neumannn和Morgenstern之期望效用之上的「SEU」[9]。歷經數十年發展而形成修正主觀期望效用模型的研究[10,11]。有鑑於此，本研究將深入釐清各種風險狀況下的決策行爲模型與風險評估的可操作性[12,13]，並參考Abdellaoui的免參數方法(Non-Paramemter Method)[14]導出效用與機率加權函數，期望能更合理地評估人類在風險狀況下的決策行爲。最後，對上述二者加以整合ISO17799資訊安全標準，從而建構兼具信度與效度的醫院資訊安全風險管理架構，期盼能對國內醫療院所推動資訊安全風險管理工作，提供具體的建議與改善方法。

## 材料與方法

本研究以中部某醫學中心推動資訊安全風險管理計畫爲個案進行實證分析。研究設計分爲規劃、執行、控制、流程回饋與評估四個階段，醫院資訊安全風險管理研究流程圖 (圖一) 所示：第一階段根據文獻歸納醫院推動資訊安全風險管理潛在的風險類別，藉以提供執行階段所需風險情境之參考；第二階段爲整合ISO17799標準管控要項與潛在風險類別爲範疇，同時進行利害關係人深度訪談以完成風險情境建立，再以免參數方法計算個別利害關係人在不同風險情境下的效用與機率加權函數；第三階段則是進行修正風險管理模式的建構，最後透過流程回饋與評估機制進行調整與完備。研究設計流程內容說明如下：

一、**規劃階段**

爲了能周詳地檢視醫院資訊安全風險管理所涵蓋的範圍，本研究根據文獻探討並歸納醫院推動資訊安全潛在發生風險類別有：

(一) 計畫規劃的風險[15]：缺乏嚴謹的計畫規範或高階主管的支持則會發生風險，而且影響層面深遠。影響因素包含：計畫書定義不適當、缺乏高階主管支持、缺乏最終顧客的參與或支持、計畫審查程序不完整、時間規劃不恰當、預算評估錯誤、浮報預算與誤解計畫需求等。

(二) 計畫執行的風險[16]：缺乏適當管理架構、計畫管理原則不一致以及計畫執行能力不足將會發生風險，並在計畫推動時容易產生無法預期的狀況。其中影響因素有：計畫管理原則不一致、計畫管理人員能力或經驗不足、計畫執行者未能遵循規範、缺乏適當的管理原則、不充足的訓練與缺乏專業能力的員工、部門間的衝突、無法於規劃時間內完成、超出預算、刪減預算與變革管理機制不夠嚴謹等。

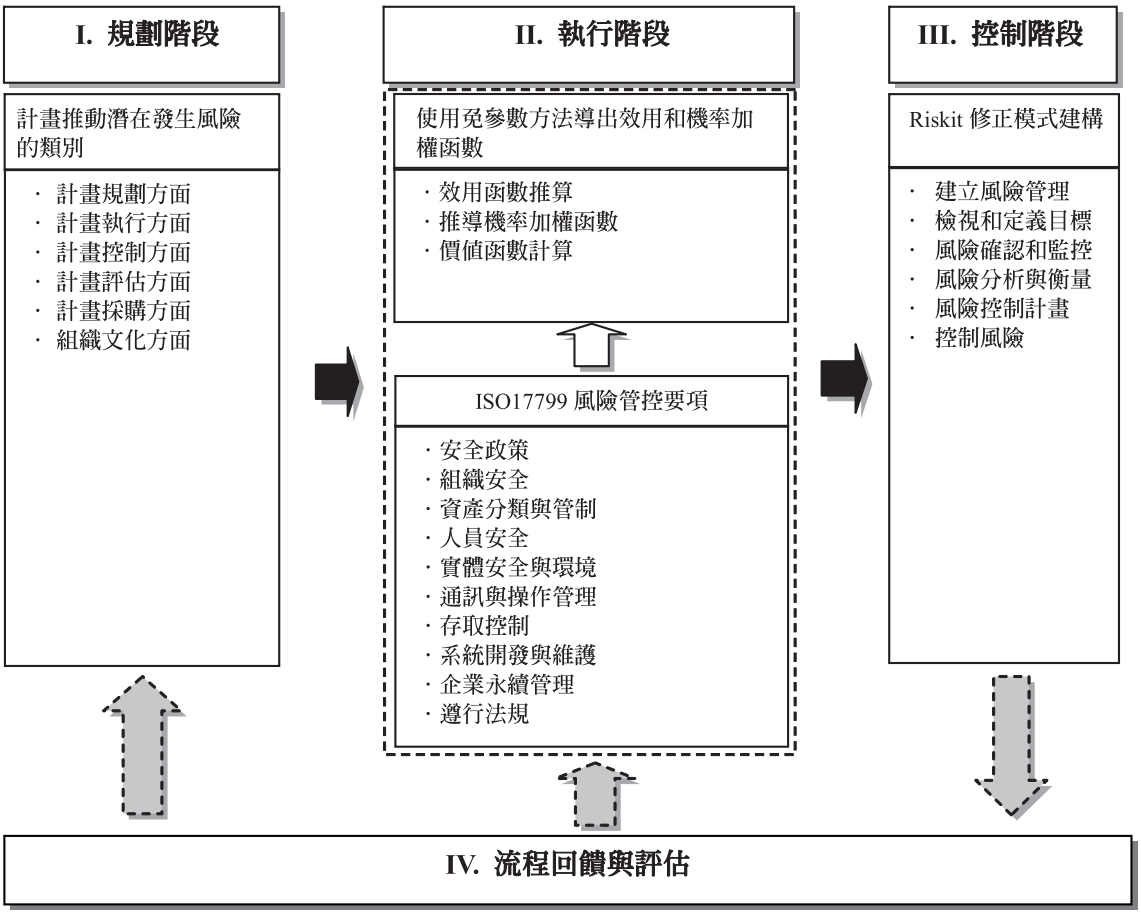
(三)計畫控制的風險[17]：缺乏適當的衡量

與定期檢核計畫或無法達成初始目標功能而產生的風險。相關影響因素爲：未能進行定期的檢核、缺乏管控機制與時間延遲等。

(四) 計畫採購的風險[18]：面臨採購法規缺乏實務彈性以及委外單位不瞭解醫院運作流程，導致問題產生時彼此信任不足。影響因素有：採購法規缺乏彈性、委外單位缺乏專業知識、醫院與合作企業存在溝通不良或不信任的狀況。

(五) 計畫評估的風險[19]：主要任務爲評估計畫是否能在期限完成、是否符合預算與達到預期的品質。影響因素包括：未能達成原訂要求的品質水準、無法於規劃時程內完成而導致放棄計畫、缺乏適當的評估方法與時間延遲等。

(六) 組織文化的風險[20]：醫院內部若無適當的溝通機制，將會因組織成員對於風險認知不同而產生風險。影響因素有：缺乏公開討論資訊安全的環境、缺乏形塑風險認知的文化以及計畫失敗消息傳播速度比計畫成功迅速等。




圖一：醫院資訊安全風險管理研究流程圖

**二、執行階段**

由於面對醫院資訊安全風險分析與衡量的問題錯綜複雜，任意處理將會造成無法預計的錯誤和損失。因此，本研究除了根據上述所歸納潛在風險發生類別外；針對實務操作的可行性，進一步導入ISO17799資訊安全管理標準，以作爲風險情境建立及其後續風險分析與衡量之規範[21]。待風險情境建構完成後，進一步再以免參數方法依序導出相依排列期望效用(Rank-Dependent Expected Utility Theory, RDEU)與累積期望(Cumulative Prospect Theory, CPT)。

免參數方法(Parameter-free)爲學者Abdellaoui所提出，其理論是奠基於相依排列的期望效用理論(Rank-Dependent expected Utility Theory, RDEU)[22,23]和累積期望理論(Cumulative Prospect Theory, CPT)[24]，並導出在金錢結果(outcome)的獲利(gain)及損失(loss)的個人效用及機率加權函數(probability weighting function)。導出的加權函數可以滿足更高或更低的次加性(subadditivity)並且與先前的參數估計研究有一致的結果。Abdellaoui[14]的作法是使用兩階段實驗研究法來進行研究，第一階段的方法是建構結果的順序並且使用trade-off方法公平的配置效用。第二階段是使用結果的順序來獲取機率的順序，並且依機率權重來公平的配置。Bleichrodt & Pinto[25]也使用類似的方法應用於醫療決策分析，獲得極成功的成果：證明免參數的方法並不僅限於金融方面的決策；本研究奠基於Abdellaoui理論的嚴謹性以及提出方法的可操作性，考量後把此法作爲風險分析與衡量的工具，係利用此法來求得各個利害關係人的損失期望效用曲線及機率加權曲線，並據以估算損失價值來完成風險衡量的工作。免參數計算公式爲[14]：

$$w^{+}\left(p_i\right)=\frac{i}{n},\ i=1,\ldots,n-1 \tag{1}$$

$$w^{-}\left(q_j\right)=\frac{j}{n},\ j=1,\ldots,n-1 \tag{2}$$

在上式(1)(2)中$w^{+}$與$w^{-}$分別表示爲獲利與損失的加權函數，並以符號相依(Sign Dependent)爲原則。再根據累積期望效用理論$p=(x_1,p_1;\ldots;x_n,p_n)$得知，其中$x_1\le\ldots\le x_r\le 0\le x_{r+1}\le\ldots\le x_n$，因此相對於獲利的決策權重$\pi_j^{+}$與損失的決策權重$\pi_i^{-}$可以公式(3)與(4)表示[12]：

$$\pi_j^{+}=w^{+}(\sum_{k=j}^{n}p_k)-w^{+}(\sum_{k=j+1}^{n}p_k)=\sum_{k=j}^{n}\frac{k}{n}-\sum_{k=j+1}^{n}\frac{k}{n}\qquad for\ j\le n-1,\ \ j=1,\ldots,k,\ldots,n-1 \tag{3}$$

$$\pi_i^{-}=w^{-}(\sum_{k=1}^{i}p_k)-w^{-}(\sum_{k=1}^{i-1}p_k)=\sum_{k=1}^{i}\frac{k}{n}-\sum_{k=1}^{i-1}\frac{k}{n}\qquad for\ i\ge 2,\ i=2,\ldots,k,\ldots n-1 \tag{4}$$

爲了消除樣本意見過於主觀與相對主觀的問題產生，本研究根據Ng, YK[26]在1984年曾經對Von Neumannn和Morgenstern的期望效用理論做出了補充，他認爲應以主觀機率爲加權來取代客觀機率。他認爲人們作決策時，是採用以心理上所感受到的機率，而導出所謂的「主觀期望效用」(Subjective Expected Utility，SEU)。進

一步提出「S」形效用函數。認爲效用函數的曲線形狀會呈現波浪狀，即某一區間爲反凹的效用函數，另一區間爲反凸的效用函數。用以解釋爲何人類同時會有賭博及保險的兩種不同風險態度的決策行爲。根據Ng, Y.-K.的論述，本研究進一步計算個別利害關係人的相依排列期望效用與機率加權函數，分別設計二階段實驗：第一階段爲建構效用函數順序實驗與第二階段機率加權函數順序實驗。首先，在第一階段係透過抵換(Trade-off)方式進行配置，意即每一情境提供兩個期望值予受測對象選擇，藉以反應受測對象的個別偏好；如圖二所示，以實驗初始損失值-15,000爲例，受測對象必須針對每一種情境的五個連續問題進行個人期望 $A=(x_{i-1},p;-15{,}000,1-p)$ 或 $B=(x_i^j,p;0,1-p)$ 選擇，其中 $x_i^j$ 爲損失結果區間的平均值，有關區間的順序則是根據第一個問題 $[x_{i-1},x_{i-1}+\Delta]$ 計算(“Δ”則表示爲一固定水準)[13]。其次，在第二階段係依據效用函數實驗所導出的結果，進一步提供問題予受測對象選擇；如圖三所示，每題的期望狀況分別表示爲 $A=(x_i,1)$ 和 $B=(x_9,1-p_i;x_0,p_i)$，其中 $x_i,i=1,\mathrm{K}\ ,9$ 表示效用函數順序實驗所獲得的風險情境結果，其中 $x_0$ 爲實驗初始值，對於區間中點值的選取方式則爲小於或等於的最大整數。有關上述實驗程序將藉由程式設計來解決樣本即時計算與無法分辨次序的問題。最後，依據所獲得樣本數據分別繪製個別利害關係人的效用曲線與機率加權曲線，進一步計算主觀期望效用價值函數以提供控制階段分析。



圖二：效用函數的實驗模型



圖三：機率函數的實驗模型

## 三、控制階段

本階段的理論基礎爲Riskit風險模式，由於該模式爲針對多數風險管理方法無法辨識風險因果關係而產生[7]。實務操作則是先透過使用腦力激盪、檢核表與目標回顧來表列風險元素與配置風險事件情境的定性分析，其次再結合效用理論予以量化計算。因此，本研究根據文獻探討並歸納醫院推動資訊安全潛在發生風險六大類別，依此類別範圍進一步以ISO17799風險管控要項加以規範，正式實驗開始前會有先導實驗，先導實驗係分別對利害關係人進行個人的深度訪談(in-depth interview)，實驗的問題係藉由與受測對象的深入訪談來完成，同時利用先導實驗所獲得的資訊發展Riskit的風險情境問題，然後加以量化成實驗問題以供受訪對象選擇，最後使用免參數的方法分別求

算效用及機率權重函數曲線。同時在實驗實施前詳細告知受試者實驗目的及實驗內容，隨後針對受試者對實驗不清楚的內容來加以講解，待受試者清楚整個實驗後，立即開始進行正式實驗。由於Riskit方法的優點在於決策者不需要具備高深的效用理論也能輕易得到風險的因果關係，然而缺點卻也是受限於簡化風險成對比較手法所造成無法解釋最終影響決策制訂的潛在因素－利害關係人互動下那雙看不見的手。因此，本研究將進一步修正Riskit模式的操作限制並加以改善。

在研究樣本的選取及其所對應職務分別爲計畫規劃者(醫學中心副院長)、計畫推動者(資訊室主任)、計畫執行者(資訊室職員)以及資訊系統供應商專案經理。因爲本研究的問題係根據先導實驗中樣本的意見來加以量化。正式實驗開始前會有個人的深度訪談(in-depth interview)，實驗的問題係藉由先導實驗與受測對象的訪談來完成，並同時利用先導實驗所獲得的資訊進行Riskit流程施測。實驗時會告知受試者實驗目的及實驗內容，隨後針對受試者對實驗不清楚的內容來加以講解，待受試者清楚整個實驗後，開始進行正式實驗，並使用實驗室實驗法，一次實驗一人，再將訪談資料彙整成風險情境，並經由專家與各利害關係人確認量化結果(表一)，才開始進行風險分析。有關風險情境順序的決定則是藉由柏拉圖(Pareto)方法將每位利害關係人對於風險情境發生機率最高與結果損失最大作爲最重要的風險情境(表二)。

表一：個案風險情境損失與發生機率估計　　單位：新台幣

| 風險情境因素 | 風險事件 | 風險反應 | 風險結果 | 估計損失 | 估計發生機率 |
|---|---|---|---|---|---|
| 1.缺乏統一的管理架構 | 管理原則不一致 | 推行單位自行尋找解決方案 | 時間延遲 | 30,000 | 0.600 |
| 2.缺乏有專業能力的員工 | 無法解決系統突發問題 | 資訊系統無法正常運作 | 無法進行風險管控 | 50,000 | 0.125 |
| 3.資訊安全系統的一致性 | 使用系統不一致 | 不同單位有傳送上的問題 | 無法達到風險管控的時效性 | 60,000 | 0.300 |
| 4.未仔細斟酌計畫時間 | 時間規劃不恰當 | 未考量到突發狀況 | 無法於規劃時間內完成 | 80,000 | 0.050 |
| 5.缺乏適當的教育訓練 | 不充足的訓練 | 無法迅速正確的推動 | 並未實際提升風險管理效率 | 100,000 | 0.400 |
| 6.缺乏高階主管的支持 | 未遵循既定規範 | 沒有依照標準作業的作法 | 並未達到風險管理目的 | 200,000 | 0.050 |
| 7.缺乏最終顧客的參與 | 計畫書定義不適當 | 沒有配置充足的時間、人力、預算 | 實際推動面臨瓶頸 | 300,000 | 0.150 |
| 8.缺乏高階主管的支持 | 部門之間的衝突 | 共同推動單位配合及參與程度不高，並相互推卸責任 | 無法順利的推動，並造成時間延遲 | 400,000 | 0.200 |
| 9.缺乏高階主管的支持 | 缺乏適當的管理架構 | 推行單位自由心證 | 未達成預期的成果 | 500,000 | 0.300 |

表二：以柏拉圖方法比較各利害關係人風險情境的順序

| | | 結果損失 | | |
|---|---|---|---|---|
| | | 高 | 中 | 低 |
| 發生機率 | 高 | 情境2 (資訊室職員)<br>情境1 (資訊室主任)<br>情境3 (副 院 長) | 情境1 (資訊室職員)<br>情境2 (資訊室主任)<br>情境1 (副 院 長) | 情境3 (資訊室職員)<br>情境3 (資訊室主任)<br>情境2 (副 院 長) |
| | 中 | 情境5 (資訊室職員)<br>情境5 (資訊室主任)<br>情境5 (副 院 長) | 情境4 (資訊室職員)<br>情境4 (資訊室主任)<br>情境4 (副 院 長) | 情境6 (資訊室職員)<br>情境6 (資訊室主任)<br>情境6 (副 院 長) |
| | 低 | 情境8 (資訊室職員)<br>情境8 (資訊室主任)<br>情境7 (副 院 長) | 情境9 (資訊室職員)<br>情境7,9 (資訊室主任)<br>情境9 (副 院 長) | 情境7 (資訊室職員)<br><br>情境8 (副 院 長) |

## 結　果

本研究主要利用免參數方法來進行修正模式的風險衡量。實驗的進行流程爲：首先，將深入訪談所發展出的風險情境予以定義及量化成實驗問題；其次，透過實驗樣本(利害關係人)對實驗問題進行偏好選擇；最後，使用免參數的方法來分別求出各個利害關係人的損失效用曲線及機率加權函數曲線。其中有關情境量化，主要是以資訊系統整合公司之專案經理所提供的資訊作爲主要基準，另外再加入其他利害關係人的意見，以形成一個合理的量化區間。在實驗的操作程序上爲每一位利害關係人各進行約30分鐘的兩個階段實驗，其內容分別爲：第一階段係利用抵換(trade-off)的方法來公平的配置效用並建構結果的順序(表三與表四)，經由獲得各實驗樣本數據後，加以繪製各利害關係人的效用曲線(圖四)；第二階段則是使用效用結果的順序$x_i$來獲取機率權重$p_i$的配置。針對實驗程序中的效用及機率兩個函數的取得，是經由一系列問題的偏好選擇來產生，並藉由「無異評價」(indifference judgment)的方式獲得所需的資料(圖五)。

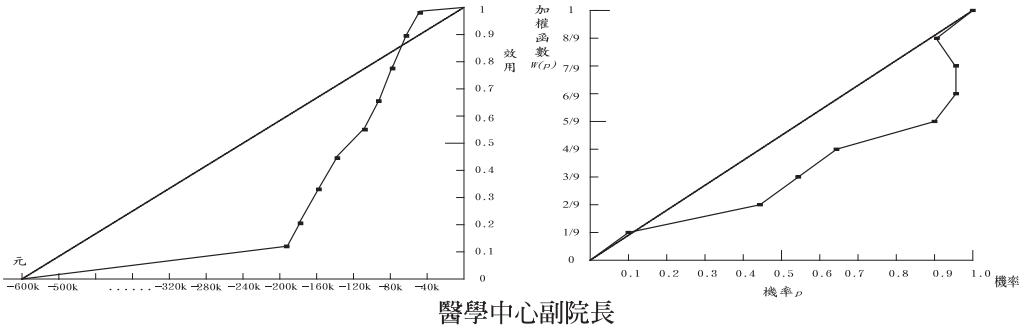
爲證明兩階段實驗所獲得樣本資料的可靠性，經由統計$\chi^2$分配檢定在第一階段實驗(p-value=0.22)與第二階段實驗(p-value=0.09)並無呈現顯著差異，證明兩階段實驗所利用抵換選擇的方法是可靠的衡量。進一步根據實驗所獲得的期望效用曲線對應專家估計的損失值(x軸)，並利用等距原理反推至效用軸(y軸)推算(圖六)，可分別求出各利害關係人的效用值$u(x_i)$、機率加權值$w(p_i)$及其對於風險情境的主觀期望效用值(SEU)，其中主觀期望效用理論價值函數的公式爲主觀效用值$u(x_i)$與機率加權值$w(p_i)$兩者之乘積(表五)。藉以提供深入分析各利害關係人對於風險情境偏好與作爲採取相關風險控制決策的依據。

表三：風險情境損失計算示例

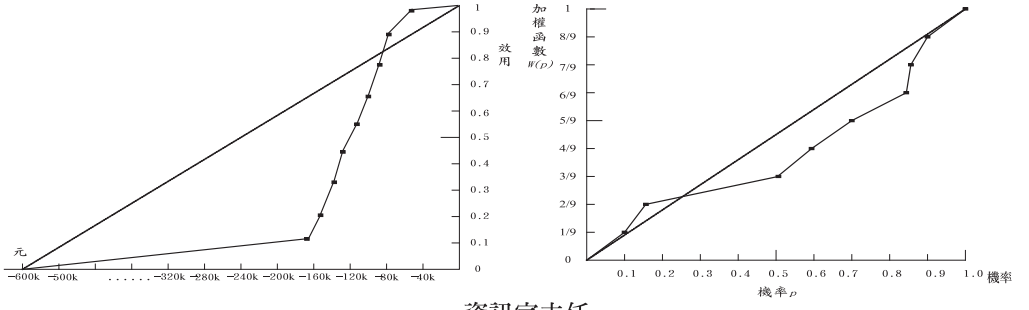
| 問題 | 偏好選擇 | 結果 $x_i$ 損失區間 | 選擇 |
|---|---|---|---|
| 1 | $A=(-30{,}000,2/3;-15{,}000,1/3)$<br>$B=(-105{,}000,2/3;0,1/3)$ | [-180,000; -30,000] | A |
| 2 | $A=(-30{,}000,2/3;-15{,}000,1/3)$<br>$B=(-68{,}000,2/3;0,1/3)$ | [-105,000; -30,000] | A |
| 3 | $A=(-30{,}000,2/3;-15{,}000,1/3)$<br>$B=(-49{,}000,2/3;0,1/3)$ | [-68,000; -30,000] | A |
| 4 | $A=(-30{,}000,2/3;-15{,}000,1/3)$<br>$B=(-40{,}000,2/3;0,1/3)$ | [-49,000; -30,000] | B |
| 5 | $A=(-30{,}000,2/3;-15{,}000,1/3)$<br>$B=(-45{,}000,2/3;0,1/3)$ | [-49,000; -40,000] | B |
| 結果 | | [-49,000; -45,000] | |

表四：風險情境機率計算示例

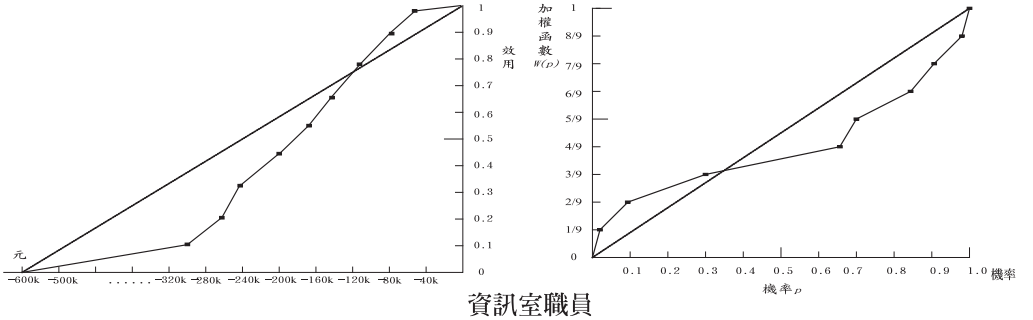
| 問題 | 偏好選擇 | $p_i$ 區間(%) | 選擇 |
|---|---|---|---|
| 1 | $A=(-47{,}000,1)$<br>$B=(-192{,}000,50;-30{,}000,50)$ | [0; 100] | A |
| 2 | $A=(-47{,}000,1)$<br>$B=(-192{,}000,25;-30{,}000,75)$ | [50; 100] | A |
| 3 | $A=(-47{,}000,1)$<br>$B=(-192{,}000,12;-30{,}000,88)$ | [75; 100] | A |
| 4 | $A=(-47{,}000,1)$<br>$B=(-192{,}000,6;-30{,}000,94)$ | [88; 100] | B |
| 5 | $A=(-47{,}000,1)$<br>$B=(-192{,}000,9;-30{,}000,91)$ | [88; 94] | A |
| 結果 | | [91; 94] | |




醫學中心副院長

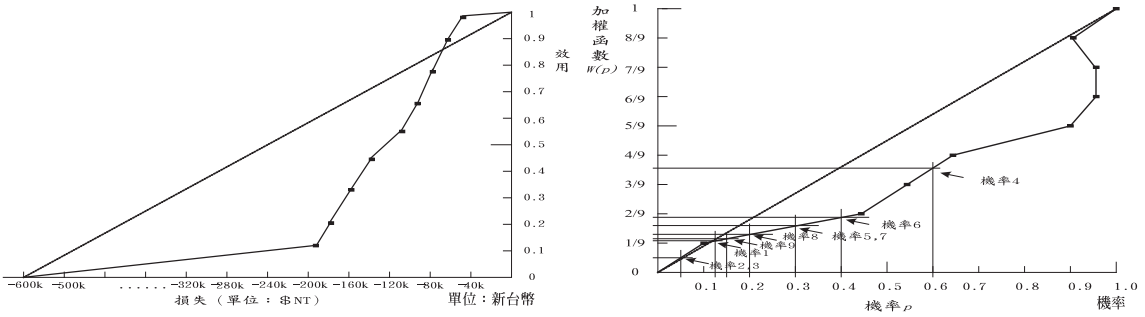



資訊室主任




資訊室職員

圖四：第一階段各利害關係人主觀效用損失曲線　　圖五：第二階段各利害關係人機率加權曲線




圖六：風險情境效用值與機率值估計方法(以醫學中心副院長為例)

表五：各利害關係人效用值、機率加權值及主觀期望效用值對照表

| 情境 | 副院長 | | | 資訊室主任 | | | 資訊室職員 | | |
|---|---|---|---|---|---|---|---|---|---|
| | $u(x_i)$ | $w(p_i)$ | SEU | $u(x_i)$ | $w(p_i)$ | SEU | $u(x_i)$ | $w(p_i)$ | SEU |
| 1 | 0.98 | 0.12 | 0.118 | 0.98 | 0.17 | 0.167 | 0.98 | 0.24 | 0.235 |
| 2 | 0.88 | 0.06 | 0.053 | 0.76 | 0.06 | 0.046 | 0.89 | 0.16 | 0.142 |
| 3 | 0.11 | 0.06 | 0.006 | 0.13 | 0.06 | 0.009 | 0.45 | 0.16 | 0.072 |
| 4 | 0.99 | 0.39 | 0.386 | 0.99 | 0.45 | 0.446 | 0.99 | 0.42 | 0.416 |
| 5 | 0.96 | 0.17 | 0.163 | 0.92 | 0.27 | 0.248 | 0.95 | 0.33 | 0.314 |
| 6 | 0.66 | 0.21 | 0.139 | 0.61 | 0.30 | 0.183 | 0.83 | 0.36 | 0.299 |
| 7 | 0.02 | 0.17 | 0.003 | 0.02 | 0.27 | 0.005 | 0.03 | 0.33 | 0.010 |
| 8 | 0.03 | 0.14 | 0.004 | 0.04 | 0.24 | 0.010 | 0.05 | 0.28 | 0.001 |
| 9 | 0.06 | 0.13 | 0.008 | 0.13 | 0.21 | 0.027 | 0.11 | 0.25 | 0.028 |

## 討　論

藉由兩種方法所獲取風險情境處理次序數據發現，各利害關係人風險值在修正模式與Riskit模式中存在顯著差異(表六)。首先，在Riskit模式中顯示每一利害關係人注重的焦點皆略有不同，其原因乃緣於其職務及其專業背景有關。以副院長(規劃者)而言，其所考量的重點爲是否有效地推動資訊安全風險管理，因此最重視的風險情境爲情境3；另外，以資訊室主任(推動者)言，其所考量的重點爲掌握計畫推動方向以及計畫是否能在期限內完成，所以最重視的情境爲情境1；最後以資訊室職員(執行者)而言，其所考量的重點爲系統能否正常的執行以及當有突發狀況產生時是否能在最短時間內獲得支援與解決，因此最重視的情境爲情境2。

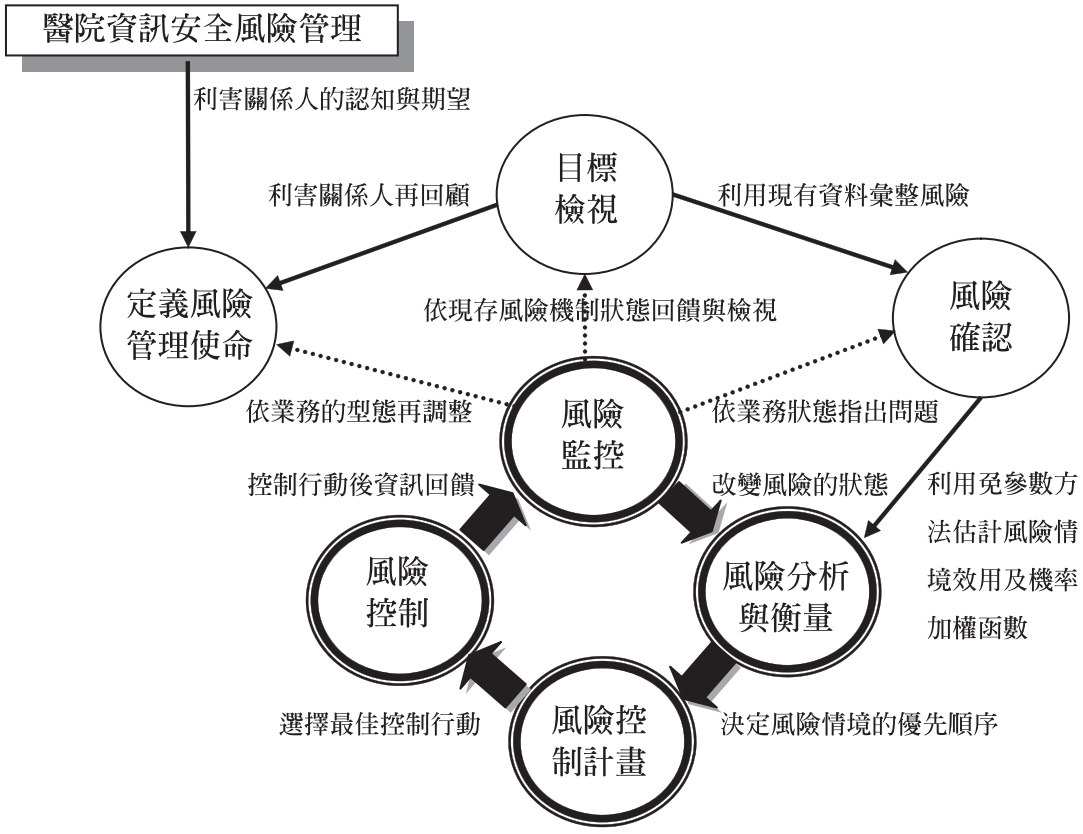
其次，從修正模式結果顯示，以副院長針對使用系統不一致的情境3爲

例，Riskit模式所排列出的風險情境爲第一，而在修正模式的期望效用值爲0.006，兩者呈現極端，追溯此風險情境在深入訪談內容，雖然副院長反映此情境有其重要性，但並不認爲會對計畫結果有嚴重影響。換言之，Riskit模式的序列效用函數雖然可以指出問題所在，但卻無法實際地反映副院長的風險態度；另外，再以時間規劃不恰當情境4爲例：Riskit模式排列的風險情境爲第三，而在修正模式的期望效用值爲0.39，以此推論該風險情境對於結果會產生重大影響，並應儘速處理爲宜。

上述分析顯示，本研究所得結果與先前學者的探討趨於一致，意即印證人類在面臨風險環境下其決策態度與行爲並非是一致的。本研究藉由修正期望效用理論的計算，在風險衡量方面確實是比Riskit的Pareto方法所使用序數(ordinal)方法的排列更爲精確與值得信賴。因爲Riskit只是將機率及損失各分爲三等分來加以排列，許多會發生的風險因素都因此被加以淡化，雖然排列出的結果都看起來很合理，但在實際上卻沒有反映出各個利害關係人的風險行爲；而就修正期望效用理論的作法而言，經由免參數兩階段的偏好選擇，可以實際反映出各個利害關係人的風險行爲，雖然排列出的方法不如Riskit的方法那麼簡單，但是爲求客觀地衡量風險的有效性，而非僅只取決於方法簡單或易用。綜合上述發現，本研究進一步提出醫院資訊安全風險管理規範與實施步驟(圖七)：

表六：Riskit模式與修正模式在風險情境優先處理次序對照表

| | | 風險情境優先處理次序 | | | | |
|---|---|---|---|---|---|---|
| | | 第一順位 (0.45-1.00) | 第二順位 (0.23-0.44) | 第三順位 (0.21-0.22) | 第四順位 (0.11-0.21) | 第五順位 (0.00-0.10) |
| 副院長 | Riskit模式 | 情境3 | 情境1, 5 | 情境2,4,7 | 情境6,9 | 情境8 |
| | 修正模式 | None | 0.386(情境4) | None | 0.163(情境5)<br>0.139(情境6)<br>0.118(情境1) | 0.053(情境2)<br>0.008 (情境9)<br>0.006 (情境3)<br>0.004 (情境8)<br>0.003 (情境7) |
| 資訊室主任 | Riskit模式 | 情境1 | 情境2,5 | 情境3,4,8 | 情境6,7,9 | None |
| | 修正模式 | 0.446(情境4) | 0.248(情境5) | None | 0.183(情境6)<br>0.167(情境1) | 0.046 (情境2)<br>0.027 (情境9)<br>0.010 (情境8)<br>0.009 (情境3)<br>0.005 (情境7) |
| 資訊室職員 | Riskit模式 | 情境2 | 情境1,5 | 情境3,4,8 | 情境6,9 | 情境7 |
| | 修正模式 | None | 0.416(情境4)<br>0.314(情境5)<br>0.299(情境6)<br>0.235(情境1) | None | 0.142(情境2) | 0.072 (情境3)<br>0.028 (情境9)<br>0.010 (情境7)<br>0.001 (情境8) |




圖七：醫院資訊安全風險管理架構

**一、定義風險管理使命**

主要任務內容爲定義風險管理的架構，並根據利害關係人的認知與期望以完成風險管理規範的策略；其產出爲風險管理架構與風險管理使命。

**二、目標檢視**

主要工作內容爲定義風險管理的範圍和頻率以及確認所有相關利害關係人，進一步釐清非風險管理標的與深入瞭解風險管理存在的限制；其產出爲5W1H(Why, What, When, Who, Where, How)明確的風險管理目標。

**三、風險確認**

主要任務內容則是以本研究所歸納潛在的風險類別與ISO17799資訊安全標準爲範圍，經由對各利害關係人實施深入訪談與確認風險；其產出爲列出風險的危害事件以及列出所有未經處理過的潛在風險。

**四、風險分析及衡量**

主要工作爲分類或整合(合併)風險以建構風險情境，同時委請專家進行風險情境損失與發生機率的估算並完成情境量化的工作，進一步利用免參數方法導出風險情境的效用與機率加權函數；其產出爲風險情境優先處理的排序與完成風險效用函數與機率加權函數曲線圖。

**五、風險控制計畫與行動**

主要內容爲計算個別利害關係人的主觀期望效用值，藉以權衡利害關係人偏好對於計畫目標達成之潛在影響，進一步篩選最重要的風險情境進行風險控制行動；其產出爲選取控制行動進行風險轉移與降低。

**六、風險監控**

主要內容爲追蹤與監督所執行風險控制行動後的情況；其產出爲風險狀態的歷程資訊。最後，透過流程回饋與評估機制進行醫院資訊安全風險管理架構的調整與完備。

## 結　論

自80年代開始，各醫療院所紛紛利用先進的資訊科技來輔助與提升醫療行政的效率，但在近年來卻有系統安全管理的問題，於是各自提出解套的方法，其中運用風險管理的構想，是最受專家與實務者們所認同的一種作法，但如何進行有效的風險管理也成爲現階段努力改善的目標。綜觀各項醫院資訊安全風險管理的經驗顯示，醫院資訊安全風險推動仍存在諸多不確定性，尤其對於資訊安全風險管理的規劃、系統的整合、預算規劃、相關教育訓練及推動的配套措施等都有略嫌不足的現況，常常造成推動單位仍須擔當問題解決者的角色。因此，若能深入調查個別利害關係人對於風險認知的態度就可以掌握不同階段潛在的風險因素，再利用免參數方法據以衡量潛在的風險事件，即使有非預期危害事件發生亦可以將風險損失加以轉移與控制，進而達成風險管理的目標。

基於本研究個案推動經驗，對於後續醫院推動資訊安全風險管理建議之實務做法：1.縮小計畫的執行規模、2.重視各項潛在風險因子與後續效應、3.訂定務實可行的計畫規範與管控架構、4.招聘及慰留優秀資訊人才，並做好各項風險知識儲存與管理、5.使用成熟資訊技術與後端支援、6.建立組織良好的風險溝通機制與文化、7.釐定組織成員的權責關係、8.納入最終顧客的角色。經過本研究的實證研究發現，相信對於建構一個更爲完善的風險管理制度之發展會有所助益，但是由於本研究僅就單一醫院進行個案探討，所以可能未盡一般化的詮釋，在此提出本研究的限制以供參考：本研究提出了一套風險管理模式，但由於需驗證提出方法的可用性，所以僅進行個案探討，希望在未來藉由更多樣本的探討進一步證明本研究所提出的方法之有效性；同時在於專家將風險情境量化的過程中，或可利用模糊集合理論把專家及各個利害關係人對於風險情境加以計算，然後再使用本研究所應用的免參數方法來進行風險衡量。

最後，本研究所提出的醫院資訊安全風險管理架構所探討利害關係人的決策態度與行爲特性具有一般性的應用價值，對於其他資訊風險管理計畫推動亦具有其適用性，可以提供其他資訊安全風險管理領域應用之參考。

## 致謝

本研究獲中山醫學大學校內研究計畫補助(CSH-2009-A-001)，特此致謝。

## 參考文獻

1. Hillbrand M, Hawkins D, Howe DM, Stayner D. Through the Eyes of Another: Improving the Skills of Forensic Providers Using a Consumer-Informed Role-Play Procedure. Psychiatric Rehabilitation Journal 2008; 31: 239-42.
2. Gomes R, Lapo LV. The Adoption of IT Security Standards in a Healthcare Environment. Studies in Health Technology and Informatics 2008; 136: 765-70.
3. Mizani MA, Baykal N. A Software Platform to Analyse the Ethical Issues of Electronic Patient Privary Policy: The S3P example. Journal of Medical Ethics 2007; 33: 695-8.
4. Paré G, Sicotte C, Jaana M, Girouard D. Prioritizing the Risk Factors Influencing the Success of Clinical Information System Projects: A Delphi Study in Canada. Methods of Information in Medicine 2008; 47: 251-9.
5. Song WJ, Cho MK, Ha IS, Choi MK. Healthcare System Architecture, Economic Value, and Policy Models in Large-Scale Wireless Sensor Networks. Lecture Notes in Computer Science 2006; 4166 LNCS: 233-46.
6. Mihalas GI. Analysis of Barriers in Implementation of Health Information Systems - EFMI Conference Introductory Address. Studies in Health Technology and Informatics 2008; 134: 21-6.
7. OECD/PUMA/SBO/RD. Management of Large Public Projects Case Studies. 22nd Annual Meeting of Senior Budget Officials 2001; Paris: 21-2.
8. Kontio J, Basili VR. Empirical Evaluation of a Risk Management Method. SEI on Risk Management. Atlantic City: NJ, 1997; 1-8.
9. Von Neumann J, Morgenstern O. Theory of Games and Economic Behavior. 2rd eds. New York: Princeton University, 1947; 164-93.
10. Matsuura N, Kamae I, Nakamura H, Maruo T. Utility and Treatment Decisions: 15 Clinical Cases in Japan. Journal of Evaluation in Clinical Practice 2001; 7: 419-30.
11. Bekker HL, Hewison J, Thornton JG. Applying Decision Analysis to Facilitate Informed Decision Making about Prenatal Diagnosis for Down Syndrome: A Randomised Controlled Trial. Prenatal Diagnosis 2004; 24: 265-75.
12. Wang, HF, Hsu, FC. An integrated operation module for individual risk management. European Journal of Operational Research 2009; 198: 610-7.
13. Abrahamsen EB, Aven T. On the Consistency of Risk Acceptance Criteria with Normative Theories for Decision-Making. Reliability Engineering & System Safety 2008; 93:1906-10.
14. Abdellaoui M. Parameter-Free Elicitation of Utility and Probability Weighting Functions. Management

Science 2000; 46: 1497-512.

15. West JC. Risk Management Information May be Discoverable. State exrel. United Hospital Center v. Bedell. Journal of Healthcare Risk Management 1998; 18: 76-8.
16. Yigit V, Tengilimoglu D, Kisa A, Younis, MZ. Outsourcing and its implications for hospital organizations in Turkey. Journal of Health Care Finance 2007; 33: 86-92.
17. Nakajima K, Kurata Y, Takeda H. A web-based incident reporting system and multidisciplinary collaborative projects for patient safety in a Japanese hospital. Quality and Safety in Health Care 2005; 14: 123-9.
18. Benn J, Koutantji M, Wallace L, Spurgeon P, Rejman M, Healey A, Vincent C. Feedback from incident reporting: Information and action to improve patient safety. Quality and Safety in Health Care 2009; 18: 11-21.
19. Hogan H, Olsen S, Scobie S, Chapman E, Sachs R, McKee M, Vincent C, Thomson R. What Can We Learn about Patient Safety From Information Sources Within an Acute Hospital: a Step on the Ladder of Integrated Risk Management? Quality and Safety in Health Care 2008; 17: 209-15.
20. Atienza AA, Hesse BW, Baker TB, Abrams, D.B., Rimer, B.K., Croyle, R.T., Volckmann, L.N. Critical Issues in eHealth Research. American Journal of Preventive Medicine 2007; 32: S71-4.
21. Thomas G, Botha RA. Secure Mobile Device Use in Healthcare Guidance From HIPAA and ISO17799. Information Systems Management 2007; 24: 333-42.
22. Quggin J. A Theory of Anticipated. Journal of Economic Behavior & Organization 1982; 3: 323-43.
23. Wakker PP. Lessons Learned by (from?) an Economist Working in Medical Decision Making. Medical Decision Making 2008; 28: 690-8.
24. Kahneman D, Tversky A. Advances in Prospect Theory: Cumulative Representation of Uncertainty. Journal of Risk and Uncertainty 1992; 5: 297-323.
25. Bleichrodt H, Pinto JL. Parameter-Free Elicitation of Probability Weighting Function in Medical Decision Analysis. Management Science 2000; 46: 1485-96.
26. Ng YK. Expected subjective utility: Is the Neumann-Morgenstern utility the same as the Neoclassical's? Social Choice and Welfare 1984; 1: 177-86.

# Developing a Risk Measurement Framework for Hospital Information Security Management

**Chi-Chang Chang[1*], Pei-Ran Sun[2], Gin-Den Chen[3]**

## Abstract

The purpose of this study was to develop a hospital information security risk framework, improve sensitivity toward organizational risk, and improve decision making. This study adopted the ISO17799, which has ten controls items, for risk management. To ensure that the proposed framework was feasible, we conducted a field study to investigate the risk to identification, analyses, measurement and control, respectively. We found that the analysis was in agreement with previous studies and that there was a great diversity in human decision behavior and uncertainty in risky environments. Thus, the proposed framework was able to elicit the real risk attitude of each stakeholder more accurately than the Riskit model. A review of risk experience was able to show clearly the potential incident through its investigation into the risk cognition of stakeholders more in detail. Furthermore, using this study, we were not only able to identify potential risk incident utilizing a non-parameter method, but also were also able to access risk and control losses. We concluded that the proposed framework can reduce information security risk about by considering stakeholders' decision positions and behavior attribute and providing decision makers the effective support need for quality decision making. Finally, the implications of the research findings can be used to investigate similar at risk decision making issues.

Keywords: Hospital Information Security Risk Management, Non-expected Utility Theory, ISO17799, Riskit Model, Non-parameter Method

---

[1] School of Applied Information Sciences, Chung Shan Medical University, Taichung, Taiwan
[2] Information Technology Office, Chung Shan Medical University Hospital, Taichung, Taiwan
[3] School of Medicine, Chung Shan Medical University, Taichung, Taiwan
[*] Reprints and Corresponding Author: Chi-Chang Chang
Address: No.110, Sec. 1, Jianguo N. Rd., Taichung, 40201, Taiwan
Tel: 886-4-24730022 ext 17107
Email: threec@csmu.edu.tw