資訊安全風險管理實務落差之探討-以某財團法人機構為例

梁德昭
淡江大學資訊管理學系
tcliang@mail.tku.edu.tw

張嘉琪
淡江大學資訊管理學系
700630279@s00.tku.edu.tw

摘要

本研究旨在探討以某採用 ISO 27001 為基礎導入資安風險管理之非營利組織對組織的風險管理是否落實並且達到有效控管，並從 ISO 31000 與現有管理方式二者之間的落差探究其原因。將 ISO 31000 與組織現有管理方式比對分析並透過專家訪談蒐集意見，從訪談結果分析歸納出組織內部對於資安風險管理認知不足及缺乏為首要主因，因此也影響主管支持程度當資源及人力較為缺乏的情況下即無法真正有效達到風險管理。期望未來企業／組織在導入 ISMS 時，能參考本研究之建議，提高組織資安風險管理認知，讓風險管理能落實於組織內部所有活動，才能有效控制組織潛在資訊風險。

This study focus on whether or not the IRM is well effectively controlled in practice, and compare their managerial activities of IRM with the requirements of ISO 31000 for a non-profit organization which has been adopted IRM based on ISO 27001. The differences of existed IRM management and the ISO 31000 standard are figured out and then raise the related issues to explore. Through the experts interview and opinions collection and analysis, results show that the mainly course of IRM is not practically effectiveness is lack of relevant knowledge of IRM organizational-wise, and thus also due to the reason of lack of supervisor support, hence also lack of resources and manpower to be put into IRM. The conclusion of this study could be as a hint to those organizations or businesses, before they are adopting ISMS, have to increase the awareness of IRM in advance, so that activities of IRM can be really put into practices to effectively control the potential information risk of organization.

關鍵詞：ISO 31000、風險管理、資訊安全風險管理

壹、　　緒論

從過去的資安事件案例大幅提升企業／組織對資安的重視，在未來企業／組織所面臨的更是嚴峻的資安環境挑戰，依據資訊資產風險評鑑並以資安治理的觀點，如何讓企業／組織在建置資安控制措施時，能在風險與成本之間取得最大效益。

目前在資安風險管理方法中，在風險評鑑與降低風險階段，需要有資安相關領域的知識，並且清楚企業運作的狀況，對於組織的決策者來說，要進行資安風險管理的決策是有困難的。(Andreas Ekelhart 2009)

本研究對象各部門推動導入資訊安全管理系統（Information Security Management System, ISMS）已有五年之久，其中風險管理又為 ISMS 主要程序之一，風險管理實施也必須要持續改進並確保整個組織的風險管理有效果及有效率。因此引發本研究對企業／組織已導入 ISMS 或是已通過 ISO 27001 認證，因企業／組織已有完整的資安管理標準，但其中資安風險管理是否適切且有效執行運作，觸發本研究第一個研究動機。

在充滿變化的時代，且環境也面臨多種不確定性及不可預測性的風險，如何以系統化的策略、程序和步驟，進行風險鑑別、分析、評估及處理是 ISO 31000:2009 風險管理-原則和指導綱要所倡導的理念並且適用於任何範圍與情況下。因此本研究對象使用的風險管理方式與 ISO 31000 所提倡的管理方式，二者之間是否有落差，其原因為何引發本研究第二個研究動機。且其差異之處的項目，是否適合納入或改善本研究對象使用的現行風險管理過程為本研究第三個研究動機。

透過以上三個研究動機，本研究將透過專家訪談，並由 ISO 27001:2005 中的風險管理與 ISO 31000:2009 風險管理-原則和指導綱要相異之處，探討當非營利組織導入 ISMS 之後，是否在組織中所有活動都已針對資安進行了妥善的風險管理。

貳、　　文獻探討

一、　風險管理

從 20 世紀開始，風險管理的觀念從美國開始傳到加拿大、英國、澳洲等國家。從澳洲／紐西蘭風險管理標準（AS/NZS 4360）的產生開始，先進國家紛紛效仿制訂全國性的風險管理標準和指引並且進行推展。影響較大且有被國際標準組織（ISO）認可的國家性標準有紐澳風險管理標準（AS/NZS 4360:1995）、加拿大風險管理標準（CAN/CSA-Q850-97）及日本風險管理標準（JISQ 2001:200l）等。(劉維義 民 97)

2009 年 11 月，國際標準組織就以紐澳風險管理標準（AS/NZS 4360:2004）為基礎，終於發佈了全球第一個一致性的標準，並將 AS/NZS/ISO 31000:2009 取代原有的 AS/NZS 4360:2004，成為風險管理國際標準。(InConsult 2009)

風險管理主要包含風險評鑑和風險控制，風險評鑑是資安管理最主要的關鍵過程，風險控制則是能確保執行資安管理是否有效(Longley 1999)。且從國外發展趨勢來看，風險管理已經成為一種趨勢，世界先進國家也都將國內外所面對的風險作為重要的政府行

政改革方向，並規劃風險管理機制及確立責任並加強風險管理的正確性及有效性。(行政院研究發展考核委員會 民 98)

二、 資訊安全風險管理

進行資安風險管理有助於組織瞭解組織內部有哪些風險存在，並且有效地進一步進行不確定性風險處理，以增進組織創造價值的能力，因此組織是需要進行一連串的資安風險管理程序。(CSCO 2004)

資訊安全管理系統（ISMS）主要程序-「風險評鑑」，資安風險評鑑又分成資訊資產識別盤點與分類、資訊資產價值評鑑、資訊資產弱點評鑑、資訊資產威脅評鑑和資安風險評鑑五個階段。(胡瑞賢 2010)

風險評鑑（Risk Assessment）是資安管理系統建置過程中的關鍵步驟，整個風險評鑑的過程就是一種：「經由評鑑後的資安政策及資安裝置的風險處理選擇，加以保護資訊資產避免遭受經由人員、設備、硬／軟體、通訊網路、作業系統等風險脆弱性而產生安全威脅的傷害。」(樊國楨 民 91)

三、 ISO 27001

ISO 27001:2005 資訊安全管理系統為目前國際公認最完整之資安管理標準，此標準可以幫助組織鑑別、管理和減少資訊設備所面臨的各種風險，這無疑的是提供組織最大的資安的保護機制。

在 ISO 27001 中也建議參考 ISO 27005 資訊技術－安全技術－資訊安全風險管理指導綱要，其可協助資安在風險管理之實作。並以風險評估理論和方法對資安進行即時且持續的監控及處理，並對發生資安事件的風險進行風險降低、風險保留、風險避免或是風險轉移等正確抉擇，其主要目的就是降低資安事件發生機率至可接受等級。

根據 ISO 27001 認證官方網站顯示，至 2012 年 8 月全球已有 7940 間企業／機構通過 ISO/IEC 27001 認證，其中前十名依序為：1.日本(4152 家通過) 2.英國(573 家通過) 3.印度(546 家通過) 4.台灣(461 家通過) 5.中國(393 家通過) 6.德國(228 家通過) 7.捷克(112 家通過) 8.韓國(107 家通過) 9.美國(105 家通過) 10.意大利(82 家通過)。(ISO)

四、 ISO 31000

ISO 31000:2009 風險管理-原則和指導綱要，它可以用於任何組織，無論其規模，活動或部門。使用 ISO 31000 可以幫助組織增進達成目標之可能性，改進機會和威脅之鑑別和有效地分配和使用風險處理的資源。

ISO 31000 不預期作為認證之目的，且並無促進組織風險管理統一之用意。使用本標準預期可用以調和現有與未來標準中的風險管理過程。(ISO 2009)

在充滿變化的時代，且環境也面臨多種不確定性及不可預測性的風險，如何以系統化的策略、程序和步驟，進行風險鑑別、分析、評估及處理是 ISO 31000 所倡導的理念並且適用於任何範圍與情況下(于樹偉 2010)。ISO 31000 強調進行風險管理之前需先納入“建立前後環節”即可掌握其目標及環境，以利未來能有效的進行風險管理，這是 ISO 31000 與其他管理機制最大不同的特點。其中規劃架構的內容包含風險管理基本要求事項，而執行過程提供了有效的風險管理必須具備的基礎，且在管理過程中皆需適時溝通與諮商及監測與審查的持續改善架構為 ISO 31000 最獨特的概念。

參、　　研究方法

一、　研究對象

本研究使用個案研究法，針對單一財團法人機構內部推動及執行 ISMS 為研究個案，並對部門內資安代表為訪談對象，以瞭解組織內在資安風險管理是否適切。透過本研究個案資安風險評鑑及管理步驟與 ISO 31000 風險管理過程進行比對，並且將其差異項目進行專家訪談，取得訪談結果進行內容分析資料研究。

本研究對象成立約 34 年，資本額約 7 億，目前約有 2000 名員工，共有 16 個部門。依組織編制並成立資安推動小組其資安代表資格為部門副主管、部門內資安推動代表或資深且熟悉部門內部運作之同仁由部門主管推派擔任，此小組由 12 位資安代表組成，其平均年資約 11 年。

二、　研究流程

本研究流程在研究範圍確定後，進行研究背景及動機確認，並透過風險管理等相關標準的文獻探討，開始蒐集研究個案資料及進行風險管理資料的整理比較，提出訪談問題後進行專家訪談。經初步專家訪談後將資料進行分析與歸納調整其原來訪談問題，再次進行專家訪談，最後將訪談結果進行分析提出財團法人在資安風險管理上的建議作為本研究結論。本研究流程如圖 1 所示。

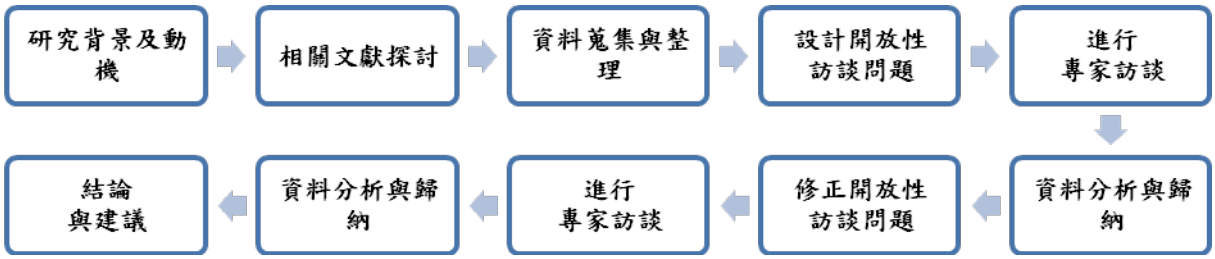

圖 1 研究流程

資料來源：本研究整理

初步專家訪談名單是透過部門有導入 ISO 27001 及未導入 ISO 27001 部門分群後隨機抽樣選出 2 位，進行初步訪談。初步訪談結果分析並修正開放性訪談問題後，隨機抽樣全部資安代表選出 5 位為受訪對象，其平均年資為 7.8 年，再次進行專案訪談，最後將訪談結果進行分析提出本研究結論與建議。

肆、　　研究分析

透過以紐澳風險管理 AS/NZS 4360:2004 為基礎，轉而發展出全球一致性的 ISO 31000 標準，因此將 ISO 31000 此標準與本研究之資安風險評鑑及管理進行比較。

ISO 31000 指出在風險管理的過程須為管理必備的一部份，且需深植於企業文化與實務內，及需配合組織的業務過程量身打造的一種管理活動。過程其包含如圖 2 溝通與諮商(5.2)至監測與審查(5.6)所述之所有活動。

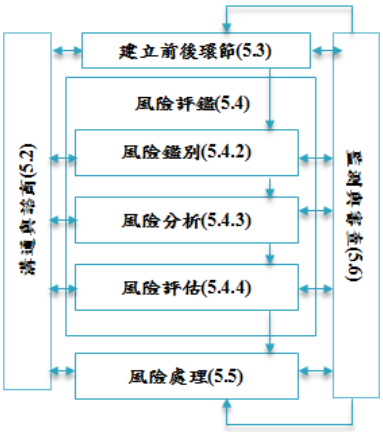

圖 2 ISO 31000 風險管理過程

(ISO 31000 風險管理過程[10])

本研究執行 ISMS 過程，其中資安風險評鑑及管理執行步驟如圖 3，此管理執行步驟是透過 ISO 27001 的管理流程參考訂制而成，其可符合本研究對象目前各部門在執行 ISMS 上是可推動及可執行為原則，其分為 1.資訊資產辨識到 4.風險管理。並透過 ISO 27001 檢核表與本研究執行 ISMS 管理過程進行調整制訂為本研究的稽核項目。

圖 3 本研究資訊安全風險評鑑及管理步驟

資料來源：本研究整理

本研究執行 ISMS 管理過程與 ISO 31000 將其項目進行比較，其比較示意圖如圖 4。

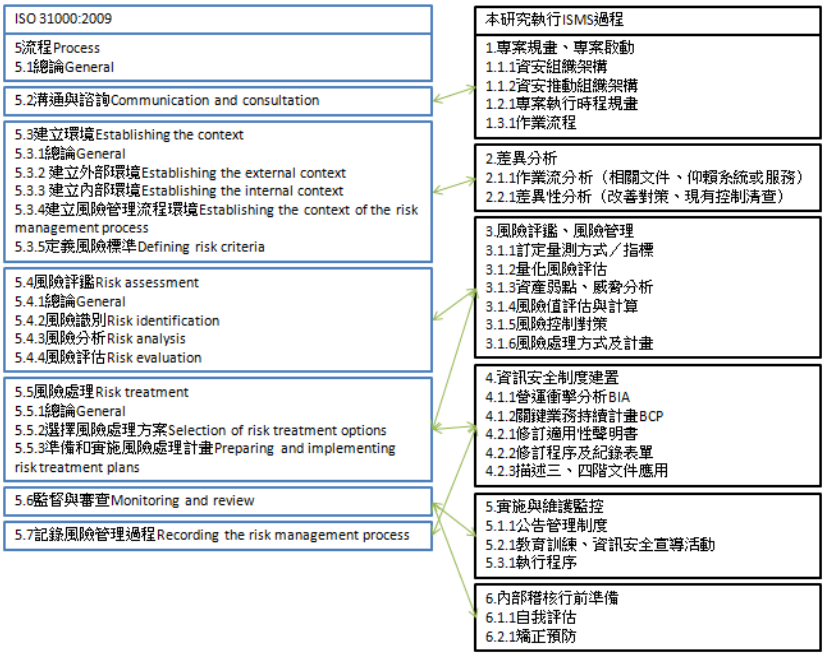

圖 4 本研究執行 ISMS 管理過程與 ISO 31000 執行項目比較示意圖

資料來源：本研究整理

一、 設計開放性訪談問題過程-各管理項目比較

（一）溝通與諮商

ISO 31000 風險管理過程第一步為溝通與諮商，且在風險管理過程的所有階段中，皆須與內部及外部利害相關者進行溝通與諮商，且須在計畫早期階段就開始納入進行，以確保實施風險管理過程與利害相關者瞭解形成決策的基準及風險採取措施的理由。此項過程在本研究之資安風險管理是缺乏納入考量，其包含與內部及外部利害相關人、可影響及其所影響、抑或自認為會影響到決策與活動的個人或組織的溝通與諮商。

（二）建立前後環節環境

範圍建立包含了組織內部與外部環境，內部可影響組織管理資安風險方式的任何業務，外部則須確保其風險準則是經考量與外部利害相關者之目標與關切的事項，且對法令規章要求及特定於風險管理過程範圍的其他事項。將組織活動的目標、策略、範圍及參數或將實施資安風險管理過程建立完畢。

接下來為界定風險準則其包括風險評量尺度、界定發生可能性的機會、風險等級及風險可接受或可忍受之等級都是須予以考量。本研究之資安風險管理缺乏與外部前後環節之目標及關切事項做確認，且並未定義部門內須要納入資安風險管理的專案、流程或活動目標的大小準則，各部門資安風險管理評鑑標準也沒有訂定統一標準。

（三）風險評鑑

風險鑑別包含了風險緣由、可影響區域、風險事件產生的可能結果，並需予以建立成廣泛的風險清單，其鑑別過程是相當重要的，因為此階段若未被鑑別出的風險因素將不涵蓋在接下來的分析之內。本研究之資安風險管理則缺乏掌握相關與更新的資訊，及未考量不顯者的緣由或是結果而產生的風險。

風險分析階段涉及對其資安風險管理發展的瞭解，提供風險評估的輸入並能決定其風險是否需要進行處理，以及決定最適宜的風險處理策略與方式。考量不同風險的緣由及之間相互依賴性是需要的，同時須與決策者及事件相關者進行有效的適時溝通，現有資訊控管方式的有效性與有效率也須予以考量。本研究在風險發展分析及評估和決定資安風險是否需要處理是不夠完善的，且提供最適宜的風險處理策略與方法也不夠完整，涉及風險的原因與其正面與負面結果跟該結果確實發生的可能性也缺乏考量，在現有資安控管機制的評鑑也缺乏其有效性跟有效率的風險考量。

風險評估目的是依據風險分析的結果，並且建立哪些風險項目該進行處理及風險實施優先順序之決策。分析過程中所發現的風險等級與納入考量前建立的風險準則相互比較，可依據此比較考量風險處理的需求，唯決策者需考量的風險更廣，應包括法令規章及其它要求的決策項目。本研究之資安風險管理缺乏提供組織判斷時所需要處理及優先處理的風險準則，並且在決策時也缺乏考量更廣泛的風險前後環節及風險受益的組織除外之團體所承受的風險容忍度。

（四）風險處理

風險處理涉及由風險評鑑後的決策進行選擇單一或是多個可供改變風險及實施的過程，而且是個循環的機制。風險處理並需要決定殘留風險可接受值，若殘留風險納入無法忍受範圍內就會產生新的風險處理，因此也需要對風險處理進行有效性評鑑。本研究資安風險管理就缺乏在實施風險處理之後並沒有進行有效性的後續評鑑。

本研究資安風險管理在選擇風險處理選項時缺乏進行實施成本和產生利害之間平衡的考量，並且也缺乏考量嚴重性高但發生可能性低的風險處理成本，在選擇處理選項也較無考量利害相關者的價值和感知。雖然本研究之資安風險管理有提供風險處理優先順序計畫，但文件化較為不足且不夠完善。當進行風險處理中對於風險處理措施是否失敗或是無效也是缺乏監測，風險處理過程中的二次風險也並未納入考量。

風險處理最後階段就是準備與實施風險處理計畫，並透過風險處理產出文件內容後，經選擇的處理項目進行實施，因此風險處理計畫內的資訊須提供處理選項選擇的理由，包含預期的獲益、負責計畫及實施計畫的相關人員、建議的行動方案、所需的資源、績效的量測方式與限制、報告與監測的要求事項及時程的安排，整個處理計畫須與組織內的管理過程相互整合，並且是經過與利害相關者適宜的討論。本研究之資安風險管理即缺乏選擇風險處理的理由，並且在風險處理後的剩餘風險並未進行監測、審查及適宜的進一步處理。

（五）監測與審查

監測與審查也是屬於風險管理過程的一部份，並且需納入平日的查核與監視。監測與審查第一步即須將相關責任界定清楚，以確保達到以下目的：確保風險管理設計與運作中的控管，取得進一步資訊以改進風險評鑑，由事件變化、趨勢、成敗分析並學取教訓，可偵測外部與內部的變化並配合修訂風險處理的優先順序和能鑑別浮現中的風險。風險處理計畫的實施進度並可納入組織整體績效管理，必要時亦可對內與對外提供報告。本研究資安風險管理監測與審查的責任並未劃分清楚，因此缺乏確保風險管理設計與運作是否有效果與有效率，並在內外部環節有變化時也無法進行風險處理優先順序的調整，目前也沒有能力針對浮現中的風險進行鑑別。

（六）記錄風險管理過程

風險管理的活動是需要可被追溯的，因此在風險管理過程中，使用有效的工具進行紀錄並且能提供組織持續的學習及可再利用是必要的。雖然本研究的資安風險管理有要求產出風險管理文件項目，但對於要在持續學習上是無法再次利用，並且要求紀錄的項目也不夠完整。

（七）經過以上比較，整理出管理步驟不足或缺乏項目如表 1。

表 1 管理步驟不足或缺乏項目

資料來源：本研究整理

1.缺乏內、外部利害相關人（可影響、其所影響、抑或自認會到決策或活動影響的個人或組織）的溝通與諮商？
2.缺乏外部前後環節（組織尋求達成其目標的外部環境）之目標及關切事項確認（法令、規章、對組織的目標具有衝擊之主要推動與趨勢、外部利害相關者的感知與價值）？
3.內部特定專案、過程或活動的目標與準則不一致？

4.組織內採用的風險管理評鑑標準不一致？
5.風險鑑別缺乏掌握相關與更新的資訊？
6.風險鑑別缺乏考量不顯著的緣由或是結果（後果）產生的風險？
7.缺乏提供風險發展分析，以評估和決定風險是否需要處理及提供最適宜的風險處理之策略與方法？
8.風險分析缺乏風險原因與緣由正面與負面結果（後果）及該等結果確實發生的可能性？
9.缺乏現有控管的風險其有效性及效率？
10.缺乏提供組織判斷需要處理及優先處理的風險準則？
11.決策時缺乏考量更廣泛的風險前後環節及風險受益的組織除外之團體所承受的風險容忍度？
12.缺乏評估風險處理的效果？
13.風險處理選項之選擇缺乏考量實施成本和產生的利益之間取得平衡？
14.缺乏考量如嚴重（高負面結果）但罕見（低可能性）的風險處理可能帶來的正當，且在經濟基礎上的正確性？
15.缺乏考量與利害相關者的價值和感知及與他們最適宜的溝通方式？
16.缺乏明確清楚鑑別實施的個別風險處理優先順序？
17.缺乏重大風險處理計畫中風險處理措施是否失敗或無效的監控？
18.缺乏引進風險處理過程中可能引起的第二次風險？
19.缺乏提供風險處理選項選擇的理由，包括預期的獲益？
20.缺乏提供風險處理後的剩餘風險之本質與程度的監測、審查及在適宜時的進一步處理？
21.監督與審查的責任應清楚界定？
22.缺乏確保風險設計與運作的控管是有效果且有效率的？
23.缺乏因內外部環節之變化可能需要修訂風險處理和優先事項的變化？
24.監測與審查缺乏鑑別浮現中風險的能力？
25.風險改善方法和工具的紀錄不完整，且無明確要求？

二、 進行專家訪談-訪談過程分析

將資料整理後製作成訪談問題，且針對以下四個大方向進行開放式訪談：

・知道有此管理過程或步驟？

・您認為本機構必須增加此項管理過程或步驟嗎？原因為何？

・您認為此項過程或步驟納入本機構內部環境適宜嗎？原因為何？

・對於納入此項過程或步驟是否會產生窒礙難行的狀況？原因為何？

（一）溝通與諮商

訪談對象在溝通與諮商步驟認為應該有條件增加，並且與內、外部利害相關人溝通是需要考量若納入此要求後是否對業務有絕對性的影響。如某專案有與外部廠商進行合作來說明，若專案規模比重佔組織或部門內業務量比重較高或是規模較大是建議應該要納入與內、外部利害相關人進行溝通與諮商。

當然納入此流程後確實也是會影響專案執行進度，不過仍需與內、外部利害相關人做溝通討論後才能有一定程度的共識，目前在執行上確實也是有困難，因為增加資安管理上的溝通與諮商可能會導致專案時程延長或是影響專案結案時間等狀況，因此是需要再加以考量是否需全面納入或是採用重點式納入。

（二）建立前後環節環境

當委辦或是委託性質類型專案業主都已有要求需要將此項目納入，但屬於組織內部自行建立的專案或是屬於規模較小的專案則並沒有納入考量，因此對於自行建立或規模較小的專案就可能會產生在執行過程中或是結案前才發現有缺失，則需即時配合狀況進行修正，若重大缺失就會發生無法順利結案的風險可能性。

在規模較小的專案主要無法落實的原因屬於專案相關承辦人或計畫主持人可能對於資安風險管理相關技術或是認知較為不足或是缺乏，但若專案有另外委由相關技術人員協助，則會產生技術人員採用的標準不一致，且該如何訂下統一原則或是委由第三方公正機構認可方式執行，該採用哪種模式跟標準也都需要經過業主認可，但若需要透過第三方公正機構認可，也可能因為計畫投入此項經費不足而窒礙難行。

針對內部特定專案、流程或活動目標的大小準則不一致的現象，訪談對象認為目前無法採用同樣的準則，重點在於各專案大小屬性適用性問題，當專案規模大小、活動標的物性質不一樣，則無法使用統一的準則，該如何進行制定適合所有專案性質的準則是需要經由全組織角度考量，但前提是必須與各部門進行討論與溝通，才不會形同虛設。

組織內部能採用統一的資安風險管理評鑑標準依各部門資安代表角度在執行上是很難達成共識且落實，因為各部門資訊資產規模差異太大，評量尺度標準難以界定，若制定統一標準也需要考量是否因各部門規模大小差異而產生資安風險評鑑結果不公平的情況，將可能導致風險處理選擇無法反映實際該控制的風險項目。

（三）風險評鑑

風險評鑑第一階段為風險鑑別，訪談對象表示因審查的頻率不夠即時，次數也不夠多就會導致無法適時更新相關資訊，並且也會因為參與管審會議的相關與會者不清楚明白其資安風險管理的目的，也會導致無法正確提供相關資料，因此在初次風險評鑑不完整就會影響其後續結果，若此專案又落於高風險區域，則管審會議就無法即時發現，因此如何落實管審會議管理制度，應該適時配合專案屬性調整招開會議頻率，而不是採用固定標準流程來進行管理。

缺乏考量不顯著的緣由或是結果產生的風險，訪談對象在受訪前並未清楚上述項目之風險須予以納入考量，說明其目的後，訪談對象認為應該要將其項目納入，但若要執行確實有困難，因為專案負責承辦人大多認為配合資安風險管理是額外負擔，且會影響原有專案時程，若要宣導執行管理應該將採用正面思考，教育同仁若納入此階段將會提高組織價值或是個人價值等，當未來承接其它專案也可增加其專業能力，較為可行。

風險分析目前部門內皆採用定期報告現況，且先評估部門可投入資源才進行風險分析，但若有新設備需要導入並委由部門統一管理，才會建議需進行現況控管並提供設備查核表供填寫，但此項要求並未強制執行。

風險評估目前提供決策者的建議方案皆已納入優先處理順序的項目，但其優先處理順序的準則並無加以說明，還是由決策者自行判斷該處理的優先順序項目。

在前後環節及其他組織或是團體是否能承受的風險容忍度也無法納入考量，評估決策時多屬於與決策者進行討論時，若決策者有提出疑慮才會針對內容進行溝通與討論，目前部門在執行資安風險管理上的細膩度確實是較為不足。

（四）風險處理

風險處理是可提供一個或多個選項供決策者選擇，並將風險處理選項進行實施，在一般要求項目除了決定殘留風險程度，並對於無法忍受的風險需要納入風險處理之外還需要將風險處理的有效性進行評鑑，訪談結果呈現因每年實施風險處理的經費難以確認，因此在評估風險處理效果是有困難的，而且也會因投入的經費不足，部份資安風險管理則無法實地進行（如：黑箱演練），所以目前確實是缺乏評估風險處理的效果。

在風險處理選項是有機會尋找另一團體或是多個團體進行風險分擔，但應該是採行重點式項目納入如：產物保險，但資產的重要性或是資產的管理權是否屬於本組織所擁有，都可能會影響到要不要進行投保，可不可以投保或是是否值得投保的相關問題。

訪談對象對於在風險處理選項的選擇之後該如何在風險管理實施成本和所產生的利益之間取得平衡確實是沒有想過這個問題，以往大部份都是以現有狀況去考量是否可以實施，對於實施後所產生的效益並不會加以考量及未來發展狀況。當風險處理中對於嚴重性高但其發生風險機率低的潛在風險，若專案性質屬組織內單一專案、短期專案就難以納入考量。目前在風險處理或控制有與利害相關者有關係並且直接影響，確實也沒有事前告知，皆採用與部門主管同意授權後自行處理，但大部份利害相關者會在意的皆是他們是否可能會因此需要付出額外成本（例如：財務、設備...）或是投入更多人力，當需提高成本或人力，就會特別提出建議，因此才會進行雙方的溝通與討論。

風險處理優先順序在文件化上也確實難以經由文件資料明確清楚表達，若負責的相關人員也沒有鑑別出風險處理的重點就會影響其風險處理的選項，因此在管審會議中也會無法辨別出相關問題。不過訪談對象表示當有重大風險處理計畫都會納入管審會議中進行追蹤，但也會產生若重大風險處理相關負責人在風險處理報告中無法明顯表達或是提出缺失，在管審會議中也就較難以發現其相關問題。

在準備與實施風險處理計畫雖然有提供處理選擇的理由，但對於預期的獲益確實沒有想過這個問題，目前提供的理由都是重於在可用資源如何分配跟可以配合資源執行下的考量，對於預期獲益上是缺乏評估，如何去評估風險處理計畫且計畫是完整的在執行人力上是有困難度，因為各部門配合執行的同仁皆屬非資安風險管理專屬執行人員，所以大多都是抽空配合執行，主要還是將人力投入專業執行在資安風險管理就只能符合基本要求項目。

（五）監測與審查

監督與審查的責任目前是採用會議方式進行記錄，若認為不需要以文件化方式呈現則是採用口頭或是其它方式做記錄，仍然是以專案大小為首要考量，若是以組織角度來看責任劃分界定上確是有不清楚之處。

在確保風險設計與運作目前採用年度期初設計與規劃，但運作上是否有效果或是效率，則由資安代表做決定及提醒，也是有疏漏之可能。

內外部環節之變化可能需要修訂風險處理和優先事項的變化也要針對提供資料的承辦人是否提供完整及詳細才有可能發現並適時調整。目前也只採用現有資產風險評鑑機密性、完整性、可用性進行確認及追蹤，若承辦人提供資料不夠完整則難以發現。

（六）記錄風險管理過程

風險管理過程是需要可被追溯，而且需要可以提供後續做學習跟再利用，目前本研究之資安風險管理在推動上並沒有全面強制要求，因此部份過程記錄就容易被忽略，且也無強制要求各部門需要通過 ISO 27001 認證，所以推動上指派的資安代表及相關負責人也都為非專職資安風險管理人員，因此在執行上能投入的人力及時間也較為不足，大部份都是利用剩餘工作時間配合完成基本要求，因此在文件化上就難以完整記錄，要強制要求也較為困難，若決策者較為重視跟願意投入較多資源，則能符合要求項目程度就會比較完整。

三、 初步訪談研究重要發現

初步訪談問題設計採用風險管理流程進行規劃，因此大部份問題及問向都有重疊及相依性，經過初步訪談資料分析後，發現依流程設計的問題優先順序反而會形成訪談對象一直重覆回答類似問題，因此造成訪談對象的困惑和產生不耐煩感。經由此發現，將重疊及相依性問題重新調整設計並整合問題。

另一發現為研究生在訪談前會先提供本研究資安風險評鑑管理現況與 ISO 31000 的差異比較並予以說明，在正式訪談前讓訪談對象能清楚本研究機構目前管理上與 ISO 31000 管理要求不足及缺乏項目，但因此也影響到訪談對象的預期心理而產生訪談對象的訪談結果不夠確切及真實。也因為對不足或缺乏項目認知不同，訪談對象會認為部門內其實已經有執行不足項目而產生誤解，反而掩蓋目前執行過程中不足之處，相較之下也會影響導入程度上的落差，導致訪談結果與現實面有所差異。

針對初步訪談研究重要發現，並配合管理流程且相依性較高的問題重新組合，將進行訪談問題題目修正如下：

（一）將各項與認知有關之問題一次整合，並優先詢問，以避免後續問題影響訪談對象的認知，因此調整為：是否清楚資訊安全風險管理需納入與內外部利害相關人溝通與諮商、外部環境之目標及關切事項確認（如：法令、規章...）、風險評鑑過程需掌握相關與更新的資訊、縱使風險後果可能不顯著也需考量？

（二）針對監測與審查中需要進行的控管跟責任問題也整合，以清楚知道各部門管審會議角色的定義跟執行項目，分別為以下二題：

1. 監督與審查的責任有清楚界定嗎？
2. 管審會是否有控管風險設計與運作中的有效果或有效率的？是否會因內外部環節之變化，而評估可能需要修訂風險處理和優先事項的變化？

（三）在初步訪談中，多數風險管理項目如：建立前後環節環境、風險評鑑、風險處理、記錄風險管理過程，訪談對象皆反映為人力資源不足、推動經費不足、沒有強制要求等等，因此對資訊安全風險管理推動整體的態度及觀念予以納入詢問：本機構資訊安全推

動為內部要求，且無要求申請通過 ISO 27001 認證，因此在資訊安全風險管理上是否因此容易被忽略？或是並不需要資訊安全風險管理？或是其它原因？

（四）將風險管理的標準與目標範圍合併處理：組織內採納的風險管理評鑑標準（如：風險評量尺度）及內部特定專案、過程或活動的目標不一致，是否認為需要統一？

（五）將內外部利害相關人與溝通與諮商相關之問題合併，以降低重覆回答的情況並增加建立溝通協商機制是否有困難，調整後為：資訊安全風險管理過程中納入與內外部利害相關人溝通與諮商（包含其決策、活動、風險處理選項之選擇）是否有困難？會因此影響專案時程嗎？如果需要是否可以建立內外部溝通與協商之機制？

（六）風險分析依執行流程順序調整，以降低訪談對象對風險分析流程執行順序產生困惑，以下二個題問題分別為：

1. 風險分析過程中是否知道瞭解風險的發展？在評估和決定風險是否需要處理時，可提供最適宜的風險處理之策略與方法？且過程中已納入的風險原因或結果不管為正面或負面發生的可能性分析？（風險降低、風險保留、風險避免或是風險轉移）
2. 風險分析過程中是否有將現有控管的風險其有效性及效率都納入？是否對多重結果或可影響多個目標加以考量？

（七）風險評估項目調整為同一題同時詢問：風險評估是否有提供組織判斷需要處理及優先處理的風險準則？決策時是否有考量風險前後環節及風險受益的組織以外之團體所承受的風險容忍度？

（八）風險處理分別針對處理前、處理中及處理後三項過程，調整題目順序讓訪談對象更清楚目前不足及缺乏的項目，三個題目分別為：

1. 風險處理選項是否提供處理選擇的理由並有考慮過與另一個團體或是多個團體進行風險分攤（如：契約與風險資金提供）？是否有考量實施風險處理的成本與可產生的利益之間的平衡？
2. 風險處理過程中是否有加以監控及對風險處理可能產生的第二次風險之監測和審查，並在適宜時的進一步處理？
3. 風險處理後是否會再對殘餘風險再進行風險處理（符合：規劃-執行-檢查-行動 Plan-Do-Check-Act, PDCA 精神）？

（九）最後為記錄風險管理過程，因此項目為所有執行過程皆需要予以執行的項目，所以保留單獨詢問：風險改善方法和工具是否有完整的執行？有明確要求紀錄？

四、 訪談研究結果

透過以上調整，並產生新的訪談問題，再次進行專家訪談，訪談結果如下：

（一）是否清楚資訊安全風險管理需納入與內外部利害相關人溝通與諮商、外部環境之目標及關切事項確認、風險評鑑過程需掌握相關與更新的資訊、縱使風險後果可能不顯著也需考量？訪談結果為若有合作關係即會相互影響。因此若外包廠商因管理不當，相對也會受到影響，就需要進行考慮。以往皆屬於被動管理，並不會去主動瞭解狀況。但現在有個資法要求，對委外廠商勢必要進行管控，並確保委外廠商是否有符合相關規定

進行執行。若針對供應商評鑑是不是要把供應商評估條件加入，目前執行上是有一定困難，若需要納入需要有一定的導入期間。

（二）監督與審查的責任有清楚界定嗎？反應出是有必要界定清楚，但是部門內並沒有內審機制，若其中有部門沒有確實執行，依全組織角度只能全面承擔，最多就只究責為什麼部門內部管控沒有確實執行，內部管審制度不夠健全。目前主責部門也沒有被授予那麼大的權責跟能力去說服各部門配合執行，只能讓各部門自行管理，但實際上需要從全組織的角度去監督其執行狀況是否有需要調整跟改進的機制。在跨部門的專案或是作業流程中即會產生無法控管或要求其它部門的執行狀況。

（三）管審會是否有控管風險設計與運作中的有效果或有效率的？是否會因內外部環節之變化，而評估可能需要修訂風險處理和優先事項的變化？目前採用每年度階段性任務，因此資安風險管理是一直不斷的運作中，但執行是否有效果是目前也都採用經驗法則進行確認，如目前需配合現行個資進行管理，管審會才會進行檢視及資源調整。風險評估可能需要修訂風險處理和優先事項的變化，目前有制度但本身面臨到新增的個資管理相關問題要納入是有困難的，因此在全組織大環境下還無法制定出明確的標準，就只能從各部門做起，只能以各部門的角色去分配有限的資源跟執行優先順序，由部門執行才能全面性知道哪裡有需要再調整跟有風險需要控管的地方。

（四）本機構資訊安全推動為內部要求，且無要求申請通過 ISO 27001 認證，因此在資訊安全風險管理上是否因此容易被忽略？或是並不需要資訊安全風險管理？或是其它原因？訪談結果顯示組織的角度如果將通過 ISO 27001 訂為各部門資訊人員或負責人員的年度達成績效目標，若是前期建置階段採用此手段是個可行方法，但對於長期後續管理未必是有效的管理方式。未通過 ISO 27001 認證與資安風險管理是否會被忽略也是兩回事，因為有通過 ISO 27001 也不一定代表組織在風險管理上已是有效的管理。訪談結果也呈現風險管理是比通過 ISO 27001 還要重要，重點是在同仁是否清楚若沒有落實資安風險管理會有什麼風險產生，且會遇到什麼困擾，當組織達到認知一致，且有風險管理共識，才能真正把風險降低，並且進行有效的管理程序修定，以降低同仁在執行管理上的問題。目前缺乏的原因是因為同仁對風險管理並不認同及對於風險管理的重要性沒有感覺，大部份都專注在自己內部的專案執行，除非是特殊專案另有要求。當組織沒有認知風險管理的重要，不管做什麼要求，都只會覺得要求項目不重要只是額外的負擔，同仁就只會選擇簡單或是較小的範圍來執行導入，所以是否有這個認知及觀念想要導入風險管理是相對重要。

（五）組織內採納的風險管理評鑑標準及內部特定專案、過程或活動的目標不一致，是否認為需要統一？目前組織內沒有統一標準是有難度，因為各部門業務型態不一樣，差異太大也太過複雜，如研究型部門跟推廣型部門重視的項目及要求等級就不一致。因不同的業務型態，要統一相關標準是相當困難，但各部門都期待組織內能夠統一標準。在推動上雖然不容易執行，但能有一致性的標準及目標，各部門才能知道組織考量及重視的標準是什麼，不過就目前狀況統一也可能會產生無法執行的情況。

（六）資訊安全風險管理過程中納入與內外部利害相關人溝通與諮商是否有困難？會因此影響專案時程嗎？如果需要是否可以建立內外部溝通與協商之機制？此項要求難

度很高，因為進行組織內部的利害相關人溝通與諮商比較容易且勢必需要溝通，但外部則有難度，通常只會告知業主如何協助計畫避免風險，外部除非有契約關係。若是委託關係則採用契約來約束，但若外部廠商又再進行第三方委外，契約上也無明確寫明，則難以掌控也無法進行要求。目前是需要能建立完善的溝通平台，且需要有一定層級的主管領導，因為各部門代表立場皆站在部門角度去思考，管理制度領導者需要有一定能力能協調及管理。在各部門的本位主義下要有共識困難度也很高，各部門因執行業務型態差異性太大，觀念也差很多，且各部門內也分別會有好幾項目標需達成，如何達到一致的標準跟目標，是領導者需要考量的。目前因組織內認知不一致，而也產生部份部門認為一定要納入資安風險管理，也有部份部門認為不需要全面納入，就本組織性質因為目前觀念認知不一致，需要多次溝通協商且觀念一致，才會有正確方向及目標要達到落實風險管理才會成功。

（七）風險分析過程中是否知道瞭解風險的發展？在評估和決定風險是否需要處理時，可提供最適宜的風險處理之策略與方法？且過程中已納入的風險原因或結果不管為正面或負面發生的可能性分析？每年都是既定的風險決策方法，且因每年度資安風險管理的組織成員變動，各成員的認知都有落差，若不清楚執行過程及管理方向，大部份都會依循原本的標準重新評估，因此容易忽略新的作業流程，或是新的業務轉變，若仍採用同樣策略就會產生問題。如何使原有成員與新成員減少交接後的落差，是本組織目前所缺乏的，整個觀念的養成是相當重要，也是必要的。

（八）風險分析過程中是否有將現有控管的風險其有效性及效率都納入？是否對多重結果或可影響多個目標加以考量？目前確實沒有納入，雖然都有依照流程進行管理，但大部份為重複項目，實際現有控管項目的有效性和是否有效率確實有遺漏。現在的表單缺乏搭配，執行者並不會拿表單與相關程序書進行比較，若要增加此項控管會比需要重頭規劃還要容易納入。

（九）風險評估是否有提供組織判斷需要處理及優先處理的風險準則？決策時是否有考量風險前後環節及風險受益的組織以外之團體所承受的風險容忍度？此項是需要被執行，但因為目前各部門資安代表認知並不一致，當資安代表也不清楚各專案或業務的風險，那就未必能提供正確的風險處理報告及風險受益的組織以外之團體所承受的風險容忍度。若跨其它組織或部門，這種狀況就會更加明顯。訪談結果呈現相關人員都需要建立風險管理的觀念。對於考量風險受益的組織以外的團體所承受的風險容忍度，取決於本組織在專案上的角色是否有足夠的談判能力，對於廠商也會自行管控包含成本等評估。重點會是在組織內風險分擔的程度比例。

（十）風險處理選項是否提供處理選擇的理由並有考慮過與另一個團體或是多個團體進行風險分攤？是否有考量實施風險處理的成本與可產生的利益之間的平衡？如何評估該投保的是價值風險還是法律責任，如果是針對一個流程或是一個系統進行投保，對於其它系統還是會有缺失。對於重要且有投保的系統，系統本身又在資安已經做到一定程度，系統權限控管也良好，雖然資產價值很高，但整體風險是相對來的低，就沒有投保的必要性。但若對於沒有投保的系統產生了違法的行為還是會造成本組織一定的賠償責任跟問題。該如何從風險價值高的資產進行保險，或是針對特別的業務、流程、系統

或是資料庫進行各別保險是比較可行的，但必需先進行全組織資產價值評估跟責任問題釐清。

（十一）風險處理過程中是否有加以監控及對風險處理可能產生的第二次風險之監測和審查，並在適宜時的進一步處理？風險處理後的剩餘風險確實沒有執行，如每年度定期的教育訓練，教育訓練前有進行預估可以降低多少風險，但實施後並沒有評估教育訓練項目是否有確實降低風險，在有效性評估並沒有執行。

（十二）風險處理後是否會再對殘餘風險再進行風險處理？對於風險處理後的剩餘風險進行監測、審查及進一步處理，目前執行上是有困難只能每年重新規劃全年度教育訓練項目，但無法針對單一教育訓練項目實施後的檢討。

（十三）風險改善方法和工具是否有完整的執行？有明確要求紀錄？目前有文件化的紀錄，但對於資安相關的教育訓練，都是採用使用者的角度進行訓練或是設計相關程序書及文件，但其實使用者並無法知道真正風險管理的原因，會產生資安風險管理基礎認知的不足。訪談結果認為除了對一般同仁 ISMS 邏輯的教育訓練，也要特別為參與成員進行種子訓練，才不會造成參與成員無法清楚瞭解組織的目標，當然主管的支持及資源投入也是相對重要。這不單單透過文件化就能夠完全傳達。記錄是證據的保存，但無法靠文件化就可以讓未來要負責的同仁能清楚且可執行。雖然文件化提供了檢討的功效，但如果對於新手該如何有效的執行及持續運作，是需要考量的。當新參與成員的認知不一致，也會導致各成員提供的資訊及評估內容是不正確的。

伍、　　結論與建議

一、　結論

透過 13 個訪談題目結果分析，有高達 9 個題目訪談對象多數認為組織內部對於資安風險管理認知上是不足及缺乏的。雖然有部份部門已通過 ISO 27001 認證且也瞭解推動 ISMS 目的，但是落實風險管理跟通過 ISO 27001 認證又是兩回事，所以認知不足及缺乏會產生組織是否有執行風險管理跟已通過認證是沒有絕對關係的，而且通過認證也無法確保對於組織內的風險是否已降低及有效控管，二者之間的落差是需要重新思考。因此組織內部對於風險管理認知是一致，且皆有風險管理共識，才能真正把風險降低及確保組織的風險管理可有效果、有效率及協調一致的管理。

結果分析也呈現主管支持程度不足高達 7 個題目之中，其主要原因也是主管對於資安風險管理上認知不足及缺乏，因此對於資源及人力的投入支持程度也就相對的較少。部份部門也因為已通過 ISO 認證，對於風險管理該投入的資源及人力也只止於可符合認證標準，但對於未通過認證的部門，主管支持程度則受限於只需要通過組織內部基本要求即可，因此在資源及人力不足有限，要落實風險管理也有一定困難。其中也表現出因組織型態差異太大，組織內部基本要求也只能符合各部門皆能執行及運作的最低門檻，所以要符合風險管理期望及目標是有其差異。

結果分析也反映出 7 個題目之中都有因為現有資安風險管理方法未明文規定其相關執行項目，各部門每年雖然有符合 ISO 的 PDCA 執行精神，但也因為現行管理中並沒有

完整制定出明確的資安風險管理標準及方法，組織內部查核項目也是採用 ISO 27001 檢核表進行制定，因此查核項目也不夠完備。尤其執行人員大多認知不足，也都屬於非專屬資安風險管理人員，造成只清楚知道配合組織內部需要查核項目進行管理，因此未載明之風險管理要求或是過程皆未落實，導致組織是無法真正有效進行風險管理。

二、 建議

本研究對象為單一財團法人，建議後續可研究其它性質之組織，對於資安風險管理的認知是否也有不足及缺乏的狀況，以加強組織風險管理觀念。

當全球已有 7940 間企業／機構通過 ISO/IEC 27001 認證，其中台灣排名為第四名，已有 461 家通過（2012 年 8 月統計資料），但對於這些已通過認證之企業／機構對於資安風險管理上是否也都有效落實於組織內所有活動之內，建議後續可針對通過認證的企業加以研究。

參考文獻

1. 于樹偉，2010，『全球風險管理發展趨勢』，永續產業發展雙月刊，第 53 期，40～47 頁。
2. 行政院研究發展考核委員會，民 98，『風險管理及危機處理作業基準』，行政院。
3. 胡瑞賢，2010，『資訊安全風險評估模式之研究—以某半導體封裝公司為例 (下)』，電腦稽核，第 22 期，1～22 頁。
4. 劉維義，民 98，『ISO 31000 風險管理概論』，永續經營雙月刊，第 40 期，3～10 頁。
5. 樊國楨，民 91，資通安全專輯之五資訊安全風險管理，台北，行政院國家科學委員會技術資料中心。
6. Andreas Ekelhart, T. N., Stefan Fenz "Automated Risk and Utility Management," *Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on*) 2009, pp 393-398.
7. CSCO "Enterprise Risk Management — Integrated Framework.," in: *the Committee of Sponsoring Organizations of the Treadway Commission*, 2004.
8. InConsult "Risk Management Update ISO 31000 Overview and Implications for Managers,") 2009, pp 1-10.
9. ISO "WebSite,").
10. ISO "Risk management — Principles and guidelines ", 2009.
11. Longley, D. "Information security management and modelling," *Information Management & Computer Security* (7:1) 1999, pp 30-40.