非營利單位資訊災難備援機制建置之雛形研究

謝昆霖
台東大學電算中心
klhsieh@nttu.edu.tw

呂易儒
南華大學資管所
csvan@seed.net

郭俊賢
台東大學電算中心
jhkuo@nttu.edu.tw

林俊男
中正大學資管所博士班
a103p2@yahoo.com.tw

石琢暐
台東馬蘭國小實習教師
gohiei@nttu.edu.tw

摘要

隨著近年來資訊科技的發展，導入資訊技術以提昇組織效率與競爭力已經是全球的趨勢。而在近年來全球資訊安全事件不斷發生，資訊犯罪手法不斷翻新，為保護組織內部資訊相關資產並保持組織持續運作，導入資訊安全管理系統（Information Security Management System ，簡稱 ISMS）便是一套可有效控制管理之方法。國際間建構資訊安全管理系統通常採用 BS7799 與 ISO/IEC17799 資訊安全管理規範為標準，以此標準來管理組織內部資訊的運用、資訊硬體的安全以及資訊使用者的控管，以達成資訊資產的「機密性」、「完整性」及「可用性」。本研究以個案研究方式，對一正以 BS7799 標準導入資訊安全管理系統之非營利機構進行訪談與實地觀察，探討其組織特質及資訊安全管理政策，並以該個案為參考來適切地規劃一個非營利機構的資訊回復及災難備援機制。

關鍵詞：資訊安全管理、備援機制、BS7799。

Abstract

Applying information technology to promote the organization efficiency and competitiveness will be the development trend in recent years. Information Security Management System (ISMS) had been known as a way to keep and protect the stable and continuous operation of the information assets for most organizations. BS7799 and ISO/IEC17799 will be the international standard frequently used to construct the information security management security for most organizations. Applying BS7799 and ISO/IEC17799 to manage the application of information, the safety of hardware and the right of users will reach “Confidentiality”, “Integrity” and “Availability” of information assets. This research uses case study technique to investigate a nonprofit organization which applying the ISMS based on BS7799 standard. The ISMS will be initially discussed, and the information recovery mechanism process will be then constructed in this study. The information assets can be protected, built and recovery at the shortest time by using the constructed information recovery mechanism process when information security events happen.

Keywords: Information Security Management, Recovery Mechanism, BS7799.

1. 前言

隨著近年來資訊科技的進步，全球企業組織 e 化的程度快速的提升，不管是企業內部文件控管、客戶關係管理、供應鏈流程控制等，皆強調必須結合資訊科技（IT）以達成快速、便利、降低成本的需求以提升企業的競爭力。當企業要運用資訊科技來提升競爭力的同時，企業對資訊科技的依賴也逐漸的在提升，這也代表著資訊在企業的價值，因此資訊安全的維護也就更加的重要。為達成資訊安全的目標，導入「資訊安全管理系統」（Information Security Management System，ISMS）已成為全球的趨勢。現今對於資訊安全的研究，大部分著重於資訊安全技術方面的研究，如：防火牆技術、電子商務安全、資料加解密的方法等技術不斷的被提出運用[3,5,6,7]。

依據林震岩[1]對我國產業界的研究，如果資訊系統停擺一小時，會有 39%的公司發生核心活動全面停擺的危機；如果資訊系統停止二至三周，將會有 88%的企業將全面停擺無法運作，僅有 4%以下的公司還可以利用人工作業來維持公司的運作，由此可見資訊安全事件對於企業維持營運的重要性。因此，當資訊安全事件發生時，最重要的是如何在最快、最短的時間內恢復企業的運做以降低損失，並提升企業競爭力。資訊系統導入國內的企業已漸漸成為全面的趨勢，但是由於資訊安全管理發展時間不長，大部分已導入資訊科技的產業對資訊安全的管理面的認知並不多；由美國聯邦調查局 FBI 的統計調查顯示出在資訊安全中，有 65%的攻擊是來自於組織內部疏失及操作失當，通常都造成資料損毀或遺失[2]。本研究將藉由訪談目前正在以 BS7799 資訊安全管理規範導入資訊安全系統的非營利之公務機關，由文件分析及訪談法來探討其回復流程及災難備援機制，並針對該機關現行組織與系統間相互調適之情況加以修改流程，以改善其回

復作業。希望藉由新的技術與觀念來建立一套能適用於非營利單位之資訊安全備援機制，並進而建立組織內部緊急應變流程，使組織遭遇資訊安全事件時能夠快速的應變，減低組織的傷害，以達成永續運作的目標[14, 15, 16]。

2. 文獻探討

2.1 國際資通安全管理標準-BS7799

BS7799 全名為 BS7799 Code of Practice for Information Security，是由英國國家標準協會（British Standards Institution，BSI）所制定之資訊安全管理系統標準。其前身為 1993 年英國工業與貿易部依據世界經濟發展組織（Organization for Economic Cooperation and Development，OECD）的「資訊安全指導方針」為基礎所頒佈的「資訊安全管理實務準則」。1995 年 2 月英國國家標準協會將「資訊安全管理實務準則」修訂後訂定為英國國家資訊安全管理系統標準 BS7799 第一部分，並於 2000 年 12 月通過 ISO 國際標準組織審議，成為 ISO/IEC 17799 國際標準。BS7799-1 是組織建立、實施資訊安全管理系統的一個指導性準則，主要目的是為組織提出一套實施資訊安全通用的標準，它提出十大管理要項、36 個控制目標以及 127 個控制項目，共分為十二個章節。BS7799-1 主要著重在風險管理，目的是協助組織預先規劃安全政策，並協助各個不同的組織找出所有控制項目中適用於組織相關業務的部分。BS7799-2 建構的資訊安全管理系統依循著 PDCA（Plan-Do-Check-Action）循環模式來持續進行改進，以達成建構完善的資訊安全管理系統的目標[4]。PDCA 循環模式應用於資訊安全管理系統可描述如下圖 1。

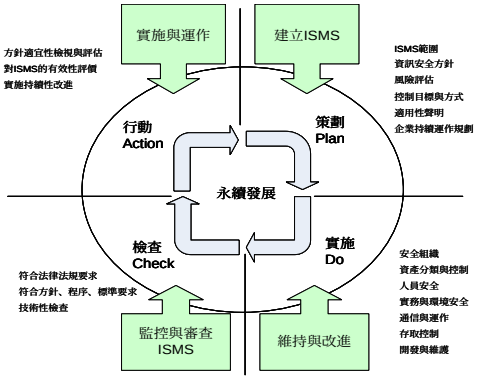

圖 1. 資訊安全管理系統持續改進 PDCA 模式（本研究整理）

BS7799 主要以十大管理要項、36 個控制目標以及 127 個控制項目為內容，下表（表 2）列出十大管理要項：

表 2. BS7799 的十大控制要項與 36 個目標內容

管理要項	
1	安全政策（Information Security Policy）
2	安全組織（Security Organization）
3	資產分類與控制（Asset Classification and Management）
4	人員安全（Personal Security）
5	實體與環境安全（Physical and Environmental Security）
6	通訊與操作管理（Communications and Operations）
7	存取控制（Access Control）
8	系統開發展與維護（System Development and Maintenance）
9	企業業務活動不間斷管理（Business Continuity Management）
10	法規符合性（Compliance）

2.2 資訊回復與災難備援

在面對天災人禍等不可知的危機發生時，大多數資訊化的組織皆無法抗拒危機以致於營運中斷，也造成了組織許多有形與無形的損失，因此可靠、安全的危機處理與備援機制對於組織的永續經營運作便成為必要性的工作。根據 VERITAS 公司針對全球資訊部門 1,259 位主管的調查（2004/3）[8]，調查結果顯示雖有高達 92%的主管認為發生災難時備援的重要性，但僅有 38%的主管充分了解災難備援（Disaster Recovery, DR）對企業永續經營的必要；而一旦發生災難時也僅有 44%的企業只採取復原或備份資料以作因應，顯然企業對災難發生時的因應，僅侷限在企業資料的回復階段，並不了解災難發生時所應進行的備援計劃，這項調查的結果令人擔憂。根據調查顯示，企業災難備援在 2002 年至 2003 年確實有明顯增加的趨勢（33%→51%）；可見備援計劃逐漸獲得企業重視。另外調查中發現災難所衍生的後遺症，以「降低生產力」最受企業重視（62%），因此發生災難時如何維持組織運作及生產才是企業採用備援計劃的首要考量。及早建置安全的資訊基礎架構以及備援回復系統，並配合資訊安全技術方面的管控，使產生危機的可能性降低，以確保組織的永續經營運作。資訊備援的方式可以「回復時間」來區分，要回復越快，則所需花費的備援設備建置成本就越高，相對的組織停止運作的時間也就越短。因此組織要建構資訊架構前需先做評估，包括衡量組織資訊系統可停止營運時間、資訊系統停止後的影響以及資訊系統運作的最低條件等，再決定組織要採用何種備援方式。資訊備援現今常分為三種類型：基本資料備援、遠端伺服器主機備援及專屬設備備援[9]。

3. 研究方法與程序

3.1 研究方法

本研究是以BS7799資訊安全管理規範探討組織建構資訊備援系統流程。由於資訊安全管理系統發展的時間並不長，而且我國企業對於資訊安全管理中備援機制的認知並不完善，因此本研究藉由B機關的個案來探討備援機制的重要性並建構其流程。因本研究可探討的個案數目並不多，因此參考高層主管安全意識及環境不確定性對企業資訊安全活動成效之影響[10]、資訊安全管理系統的導入與管理模式[11]等研究，採用「質性研究法」中的「個案研究法」進行研究[12, 13]，並採取訪談法與文獻內容分析法蒐集個案組織的資料，希望藉由這個方法與研究對象進行溝通，並透過與資訊安全人員進行訪談後以改善個案組織的現行備援行動。以下進行個案研究法與訪談法操作方式與限制之了解。

3.2 研究對象

本研究所需之研究對象必須有獨立之資訊單位、需為正在導入或是已導入資訊安全管理系統、其導入資訊安全管理系統是以 BS7799 為基礎架構、資訊來源需為多元化的（即時資料、委外資料、固定時間進入的資料）。經由上述條件比較後，本研究選擇之B機關為一非營利機構，並正以BS7799標準導入資訊安全管理系統，資訊單位內含有機房，並同時具有各種不同來源的資料。B機關的各種條件皆符合本研究之需求，本研究將透過訪談B機關資訊安全人員以瞭解其資訊安全運作狀態，並瞭解其組織文化，以建置符合研究對象之資訊備援回復系統。

3.3 訪談大綱與說明

為了能夠完整的了解研究對象之現實狀況，本研究將針對研究對象之資訊安全人員做一對一訪談，以得到本研究所需之重點資料。訪談的內容大致可分為：組織背景資料、組織人員資料、組織內部運作程序、組織資訊系統未來發展與組織系統設備等。

本研究擬訂訪談大綱如下：

1. 貴單位目前是否對資訊安全人員進行任務編組？是否進行攻防演練？
2. 貴單位目前機房有那些設備？是否有進行備份措施？
3. 貴單位目前選用之作業系統為何？資料庫為何？
4. 貴單位目前是否具有緊急應變計畫與災難備援系統？
5. 由貴單位所提供之資訊系統架構圖可知貴單位目前只有將台北機房單向將資料送至台中機房儲存，未來是否計畫進行雙向備份或其他備援措施？
6. 未來貴單位之備援方式是否改變？是否考慮異地備援或委外備援？

3.4 研究對象訪談

3.4.1 研究對象背景資料

本研究之研究對象為一非營利機關，在台北與台中共有三個辦公室。其接觸資料中含有大量且高機密性資料（包含身份證字號、姓名、電話、地址及生日等資料），而其資訊部門為一任務編組機構，主要負責研究對象之資訊硬體維護、資訊安全等，並於 2003 年正式導入資訊安全管理系統。

3.4.2 組織資訊系統架構

經由實際到研究對象機房觀察後以及與研究對象資訊人員訪談後，發現研究對象內部具有 30 多部主機，並於台中及台北辦公室具有兩個機房（如圖 2），目前將主要營運系統建置於台中辦公室，台北辦公室與台中辦公室以專線連結，每日定時將資料傳送至台中機房。而台中機房目前是以磁帶作為其主要備份模式，並透過專線將資料傳送至 Hinet 進行備份。備份後之磁帶將送至台北機房進行保管，期間如無發生問題，將於二至三周送回台中機房重複使用。

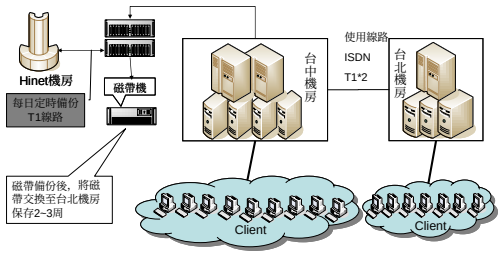

圖 2. 資訊系統架構圖

4. 訪談分析與備援機制的建構規劃

4.1 訪談結果

4.1.1 優點

1. 研究對象高層人員對資訊安全管理的推動非常支持。
2. 研究對象所採用之設備皆為知名大廠設備，相同機型並購買兩部以上，如遭遇硬體可快速替換。
3. 研究對象內部所建置的資訊系統採用多種不同的系統平台，對於資料的品質以及系統穩定性可達到最佳化的品質。
4. 研究對象對於人為因素的外在破壞（如駭客、病

毒）防範程度高，防火牆及網路皆嚴格管控。

5. 研究對象預先規畫的硬體儲存容量充裕，足以因應未來需求。

4.1.2 缺點：

1. 設備、系統及儲存備份裝置大多數集中於台中機房，雖然管理方便，但風險集中。
2. 系統多元化雖為優點，但也導致資料量大幅度增加，對整體的管理造成負擔。
3. 研究對象的營運系統並未建置同步主機，當遭遇重大事件時，系統運作將中斷無法運行。
4. 主要備份除磁碟陣列外，採用磁帶備份，雖然磁帶具有容量大的優點，但是備份還原時間過長。
5. 雖有建置外部備援系統，但因於每日下班後才定時進行備份，如機房儲存設備遭遇問題即時資料可能消失。

4.2 資料分析

經由訪談後，本研究訪談後針對 BS7799 之十大控制目標做評估資料表，如下表 4，並可得知本研究之研究對象高層對資訊部門的態度與看法。

表 3. 訪談資料匯整表

評估要項	說明	組織內部高層認同程度	資訊單位實際執行程度
安全政策	資訊安全政策	高	高
安全組織	組織架構、運作流程	中	中
資產分類與控制	資產分類並做分級保護	中	中
人員安全	人員訓練、安全防護	高	高
實體與環境安全	設備保護及控管	中	高
通訊與操作管理	通訊設備使用及管理	中	高
存取控制	對於使用者的權限控制	高	中
系統開發展與維護	系統開發、維護程序	低	中
業務活動不間斷管理	組織永續運作	高	中
符合性	法規符合性	高	高

由上表可知：

1. 研究對象內的高階管理部門對於組織導入資訊安全管理系統及組織之資訊安全政策是非常支持的。
2. 研究對象對其資訊安全管理的運作流程及權責歸屬均有相當良好的規劃與分配。
3. 研究對象對資訊資產的分類不夠完善，對於建構備援系統造成負擔。
4. 研究對象對於人員的教育訓練非常重視，常對人員辦理教育訓練及安全教學。
5. 研究對象對資訊機房之實體環境安全保護程度高。
6. 對於網路安全方面，保護程度高，遭遇網路事件機會低。
7. 對於資料的存取方面，因內部資料需使用人員過於複雜，因此對於資料存取權的控管需加以改進。
8. 研究對象目前之備援系統僅限於資料備份，對於主機及系統之備援需立即建立，避免遭遇災難時系統停頓造成損害。
9. 研究對象現階段的備援系統架構需針對程序、設備及方法等方向進行改善。
10. 資訊安全人員對於資訊安全政策的了解程度高，但是對於技術層面的知識需再學習與加強。

當組織要保持運作不中斷以及維持資料的安全性、完整性，建立備援系統是有效的一個方式。要建立備援系統首先必須先進行資訊整合，並對組織內部資訊資產做風險管理、資產分類，對組織內部的進行財務、需求考量，以選擇要建構何種資訊備援系統及要如何建構？

4.3 備援系統之規劃

針對以上的訪談及資料分析結果可發現研究對象對機房實體安全以及網路安全皆有高度的控管，但是須對現階段的備援流程立即進行改善，因此初步規劃出一個資訊備援流程（圖 3）。

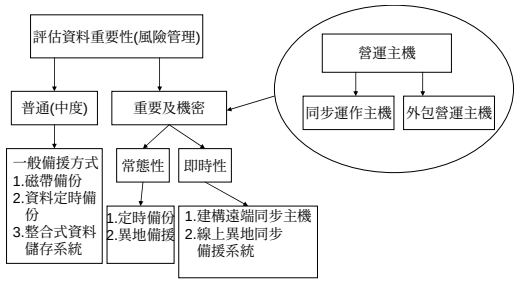

圖 3. 初步規劃之資訊備援流程圖

建置備援系統的流程可規劃為八個步驟，分述如下：

步驟一：定義系統建置的範圍：將系統要涵蓋的部分範圍設定清楚，並且以核心業務為首要建置目標。

步驟二：資訊資產分類與風險評估：將不同等級或性質的資產作分類，並且進行風險評估後以不同的方式進行備援，以節省成本並建

構最適性的備援系統。

步驟三：系統架構規劃：將系統的架構圖畫出以說明系統流程。

步驟四：確定系統建置規格及成本：將上面三個步驟所訂定的系統需求選擇最適合的備援系統，並詳盡的說明系統規格及所需成本，避免造成系統資源不足或浪費成本。

步驟五：成立資訊備援專案執行小組。

步驟六：擬定專案執行計劃。

步驟七：專案執行與系統建置。

步驟八：系統建置完成模擬演練：系統建置完成後，需在不影響營運下不斷的進行模擬演練，以達成系統不停頓的目標。

由於資訊備援的技術在近年來還持續的在不斷的更新，透過新技術可達成更完善的備援機制，但是新技術所需的費用與設備皆非常的高昂，對於一般性的組織而言是一項非常沉重的負擔，因此選擇最適合組織使用的技術與備援方式便成為重要的問題。本研究經由研究對象的訪談與文獻探討後，對研究對象內部「回復耗時目標」（Recovery Time Objective ,RTO）與「回復程度目標」（Recovery Point Objective ,RPO）做資訊備援規劃[17]。RTO 為系統完全回復運作所需時間，代表組織能承受服務中斷的時間；RPO 為資料回復的程度，代表組織可接受多少資料遺失。由 RTO 及 RPO 可以判斷組織該選擇何種備援方式進行備援。如下表 5 及圖 4。

表 4. 備援方式分析表

	備份	即時性	系統可用性	系統同部運作	RTO	RPO
磁帶備份	●				2~7 日	10~48 小時
磁帶備份/遠端回復	●		●		1~3 日	10~24 小時
資料非同步備份	●	●	●		1~5 小時	2~24 小時
異地同步備援中心	●	●	●	●	50~60 分鐘	0~10 分鐘

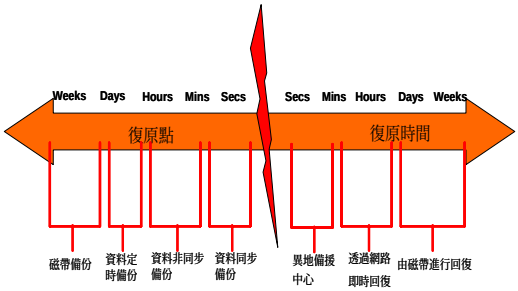

圖 4. 以 RPO、RTO 觀點選擇備援方式

對於研究對象內部一般性、常態性的資料，可使用定時、非同步的方式進行備援，將各個伺服器內的資料透過內部備份專用網路傳輸至備份主機，並在備份主機上裝設磁帶機，當資料使用磁帶機進行備份時，同時將資料透過專線或 WAN 備份至遠端資料中心的儲存主機內，並於備份完成時，將磁帶送至遠端的資訊保管中心，備份流程如下圖 5。對於研究對象內部之即時性資料、營運系統等重要及機密的資料，本研究規劃後選擇以異地備援作為其備援方式。在異地備援地點建立資料同步儲存中心與災難復原中心，在平時透過高速網路或專線將資料同步傳送至資料儲存中心；同時並建立同步運作的系統，當主機房發生災難時，可在最短的時間內由異地備援中心接手運作而不影響營運。當組織在建構異地備援中心時，需考量以下幾個條件：一、備援地點與主機房的距離要夠遠，遭遇區域性災難（如地震、火災、水災等災難）時可繼續運作。二、主機房與異地備援中心的網路必須要快速且穩定。三、儲存系統的穩定度必須要仔細考量，異地備援流程如下圖 6。

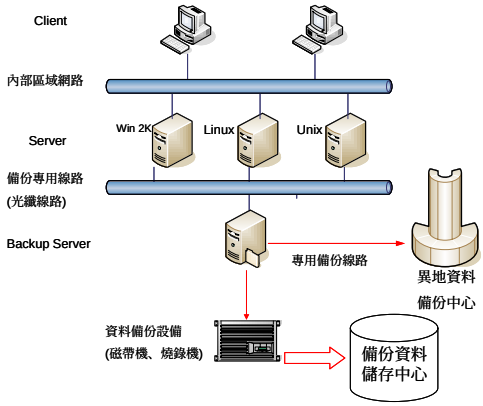

圖 5. 常態性資料備援過程

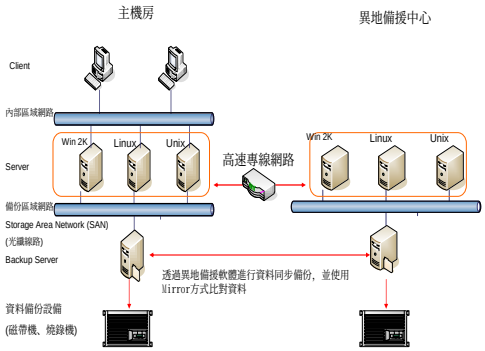

圖 6. 異地備援流程圖

由於研究對象內部營運系統包含多種類型的資料庫，且資料在進行儲存時皆會大幅占用網路頻寬，因此採用 SAN（Storage Area Network）方式，將備份主機與內部區域網路獨立分開，另外透過光纖線路建置資料儲存專用網路，以此方式可降低區域網路的頻寬負荷並可釋放伺服器資源，使主機與網路更加穩定。而在主機房與備援中心的資料備份主機透過異地備援軟體進行資料同步複製，並且採

用 Mirror 進行比對，每次在兩主機進行備份時，僅需傳送兩邊的快照資料進行比對，每次備份只傳送有異動的區塊，不需傳送重複的資料，可大幅減低資料的傳輸時間與網路的負載，並達成兩端資料的一致性及完整性。本研究將初步規劃之資訊備援流程、備援系統建置步驟與方法送交研究對象資訊安全人員討論，並且對初步規劃之資訊備援流程做更完備的修正，如圖 7。修正後的流程將資訊資產的分類以及風險、成本評估分析獨立成為兩個部份，因為這兩個部份是組織在建構資訊備援系統的過程中決定要採取何種備援方式的判斷方法；將系統的重要性、機密性以及 RTO 及 RPO 等皆做為要採用何種備援方式的考量因素。在系統建置完畢後，必須要對所有人員做教育訓練，使他們了解發生資訊安全事件時該如何做後續活動；並且不定期的對系統做穩定性測試、攻防演練以及弱點掃描分析，使備援系統能達成 99%不停頓、資料完整性的目標。

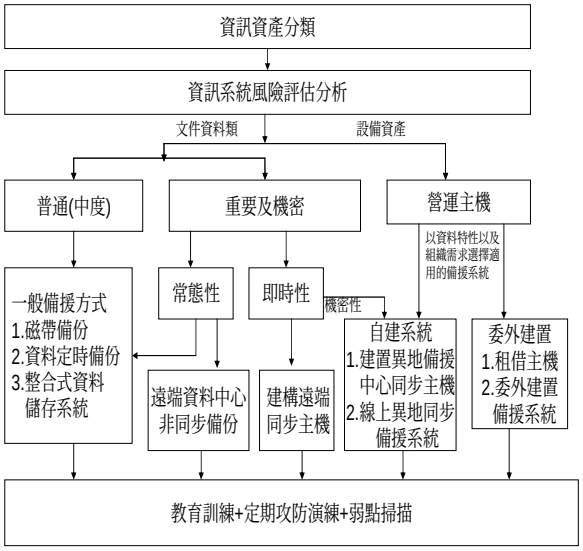

圖 7. 修正後之資訊備援流程圖

5. 結論與建議

本研究透過訪談研究對象及文獻探討後提出組織建立資訊備援系統的流程與選擇備援系統的方式，希望對正要規劃或是正在建置資訊備援系統的機構有更進一步的認知與實質上的協助。有鑑於本研究所規劃的備援流程機制正由該案機關導入實施中，相關的執行成效以及後續是否會因執行環境等未知因素的影響而需進行調整修正仍無法有相關的結果予以呈現，同時不同的公務機關可能也會因為條件、資源、考量等而有不同的思維模式，目前亦無法有效地呈現其相容性的比較。雖然有許多實際執行的成效無法適切的表現出來，但本研究所採用的解析程序以及建構的思維邏輯將可適切地作為其它相關的單位在導入及建置備援機制時可用的參考。

參考文獻

[1] 林震岩,「資訊系統與組織配合關係之研究」,國科會研究報告，1996。

[2] 徐廣寅，資訊安全管理導論，金禾資訊，2003。

[3] 行政院國家資通安全會報, 建立我國通資訊基礎建設安全機制計畫，2001。

[4] 賽克鐵門公司,「導入 BS 7799 標準─企業責無旁貸」。 http://www.symantec.com.mx/region/tw/enterprise/article/bs7799.html。

[5] 經濟部標準檢驗局，資訊技術-資訊安全管理之作業要點 CNS17799，2002。

[6] 經濟部標準檢驗局, 資訊技術—資訊安全管理系統規範 CNS17800，2002。

[7] 黃慶堂,「我國行政機關資訊安全管理之研究」,政治大學公共行政系碩士論文，1999。

[8] 資策會電子商務研究所 find 網，網路脈動，多數企業資訊系統缺乏積極的災難應變力 http://www.find.org.tw/0105/news/0105_news_disp.asp?news_id=3388。

[9] 李俊隆，論災難備援計劃在資訊安全的重要性–以美商 CTS Corporation 為例，國立中山大學資訊管理學系在職專班碩士論文，2003/6。

[10] 葉嘉綺, 高層主管安全意識及環境不確定性對企業資訊安全活動成效之影響, 高雄第一科技大學資訊管理系碩士論文，2003。

[11] 王百川, 資訊安全管理系統的導入與管理模式之研究, 中國文化大學資訊管理研究所碩士論文，2003。

[12] 通識資源網,「社會研究入門講座三：質性研究」, http://ihome.cuhk.edu.hk/~b103405/coming / qual_ seminar.htm，2001/2。

[13] 陳萬淇，個案研究法，台北：華泰，1995 年 11 月。

[14] 吳俊德, ISO 17799 資訊安全管理關鍵重點之探討，中正大學企管所碩士論文，2002 年。

[15] 林俊銘, 從企業資訊安全論備援系統的計劃與實務, 中山大學高階經營碩士專班碩士論文，2002 年。

[16] 劉永禮，以 BS7799 資訊安全管理規範建構組織資訊安全風險管理模式之研究, 元智大學工業工程與管理學系碩士論文，2002 年。

[17] Herzog Thomas（1996），朱柔若譯，社會科學研究方法與資料分析，台北，台灣：智揚出版社。