建構台灣金融產業「異地備援」生命週期檢核表

蕭瑞祥
淡江大學資管系副教授
rsshaw@mail.tku.edu.tw

鄭哲斌
台北城市科技大學資管系講師
james@mail.tku.edu.tw

賴建成
淡江大學資管系碩專班研究生
799630107@s99.tku.edu.tw

摘要

從 2011 日本東北大地震經歷，反思台灣亦是一個地震頻繁的國家，而金融服務業之資訊系統除了關係企業的永續經營與獲利外，相對於民眾而言，金融服務業資訊系統「異地備援」品質，是極為重要的，因為它關係民眾財產安全。經彙整過去研究、國際標準等文獻及與各位專家探討，並透過德爾菲法取得 44 個在「異地備援」的 PDCA 四個週期七個階段 44 個檢核項目。

利用這 44 個項目，驗證台灣九家金融服務業「異地備援」實施現況，除了確認這 44 個項目有效及必要性，並針對這九家金融服務業「異地備援」回覆資料予以分析並提出建議。

關鍵詞：持續營運、異地備援、戴明環、風險管理、德爾菲法

建構台灣金融產業「異地備援」生命週期檢核表

壹、緒論

一、研究背景與動機

1997 年 12 月 12 日於日內瓦達成金融服務業自由化協議（GATS），協議內容主要為各國要同意開放金融市場，准許外國人在相同程度的規範下經營金融事業。而我國於 2002 年 1 月 1 日亦正式成為世界貿易組織（World Trade Organization, WTO）的會員國之一，這對於台灣金融產業是充滿了機會與挑戰，在 WTO 框架底下，不論本國銀行或外國銀行，經營操作必需更具彈性，汰弱留強亦為必然之趨勢(李禮仲 2002)。而本國於 2001 年 11 月 1 日開始施行金融控股公司法，金融產業將可經由購併或跨業經營一方面降低成本，爭取競爭優勢，一方面為顧客提供更周全良好的服務，而金融服務品質卻往往是金融產業主要核心競爭力之一(楊瑞平 2005)。

2011 年 3 月 11 日 14 時 46 分（當地時間）發生於日本東北地方外海三陸沖的矩震級規模 9.0 大型逆衝區地震，並引發最高 40.5 公尺的海嘯，加上其引發的火災和核洩漏事故，導致大規模的地方機能癱瘓和經濟活動停止。而台灣是分佈三個地震帶上，平均每年約發生 18,500 次地震（其中約有 1,000 次為有感地震），而讓台灣人民印象最深刻莫過於 1999 年 9 月 21 日淩晨 1 時 47 分發生於台灣中部山區的逆斷層型地震（俗稱 921 大地震又稱集集大地震），那次造成無數人民死傷， 財產損失。除了地震之外，近年來許多天災，都有可能造成金融服務產業營運中斷，在納莉風災來時，釀成大臺北地區淹水，導致玉山銀行資訊系統無法正常對外服務，首次以林口異地備援中心對外開啟服務，這讓各金融產業深深瞭解異地備援中心之重要性。2010 年 12 月 27 日夜間 9 時，富邦產險機房火災，隔天導致產險、證券等富邦金控子公司隔天部份業務、交易無法正常運作，曝露資安危機，也對富邦金控商譽、財產等造成不小損失。在品質月刊指出，當企業如果未確實執行資訊系統備援措施，企業隨時可能發生倒閉，並對國家、社會及個人生活造成不小影響(蔡耀宗 2007)。

事實上，每個企業都瞭解「異地備援」的重要性，也都瞭解天災的不確定，但企業能做到完整的異地備援的會有多少?當要求恢復時間越短，所支出成本就會越大，反之，支出成本越少，當災變發生時，可能對企業造成營運衝擊就會越大。根據國際標準 SHARE 78(1992)將備援系統定義成七個層次中提到七種資料異地備援等級，也明顯指出，備援等級越高，所支付的費用與恢復時間呈現反比。勤業眾信月刊引用土地銀行資訊處處長認為：「資訊風險的控制與業務需求是息息相關的，在有限成本和資源下，需要透過公司高層從業務面決定那些是關鍵業務系統，再來談備援與永續經營的策略」(吳佳翰、溫紹群、黃永婷 2011)。依據 Barnes(2001)指出企業在選擇 BCM（Business Continuity Management）策略，必須權衡時間、成本及對企業衝擊，選擇一個對企業最有利的異地備援的規劃。

根據資訊產業服務年鑑(2011)提到， 資訊製造業在 2011 年在 BCM 方案的投資，將增加 8.4%，但也發現，台灣資訊製造產業對於備援設備的功能要求不夠嚴格，可以忍受一定程度資料損失。但往往企業在考量異地備援建置、規劃時，保持一種有做就好的心態，當災害發生超過原本預期時或者不是預設情境下，企業的異地備援，真可如預期般讓核心業務對外營運？依據 IThome 雜誌(2011)指出台灣企業 10 項異地備援常見缺失，在電腦稽核月刊(蒲樹盛 2005)也指出 執行資訊備援系統規劃上，常見的 5 項缺失，所以希望藉由本研究，可以與多位專家訪談，吸取專家意見及融合戴明環、ISO 31000 風險管理(2009)等多項理論及參考文獻，來建立完整一套異地備援機制，供未來金融產業在規劃、建置、維護、檢驗、持續改善之參考。

貳、文獻探討

一、異地備援七種等級

在 1992 年計算機研究組織 SHARE 與國際電腦大廠 IBM 在美國南加州阿那罕姆市（Anaheim）共同定義一套遠程災難恢復層水準方案，這樣做的目的就是為了能夠正確地描述在遠程資訊系統的災難恢復實現和量化各種成功的關鍵不同的方法任務，共定義出下列七種異地備援等級，後來業界一直沿用此標準，作為備援標準，稱為 Share78 國際標準(1992)。七種異地備援等級，層級越高，資料遺失比率就越低，系統回復時間就會越短暫，反觀，「層級 0：無異地備份」，如發生像日本大規模地震，可能企業之資訊系統將永久無法復原，對企業營運造成傷害是永久性的。

二、營運持續管理生命週期

依據國際標準 BS 25999-1(2006)定義，可以將營運持續管理區分四大階段（第一階段：瞭解組織、第二階段：決定 BCM 選項、第三階段：建置及發展 BCM 回應、第四階段：驗證、維護及自我評估）

（一）第一階段：瞭解組織和組織內、外環境

公司要建立「異地備援」制度及程式之前，要先瞭解什麼是公司所需要的，不管是從政府法令政策或利害關係人觀點等，因為資訊系統的存在目的，是在支援公司營運，而只有公司能正常營運，才能享有企業利潤的果實，從國際標準 PAS 56(1992) BCM 生命週期循環，也可以明確看出，在制訂營運持續管理政策前，可以從公司組織、文化及計畫等瞭解公司營運所需，依據 ISO 27005(2008)內容描述，組織在制訂風險管理政策，應該考量(1)支持公司資安政策(2)符合法律和盡職的證據(3)依據業務連續性計畫(4)依據事件響應計畫(5)符合該業務、服務或機制對資訊安全的要求；另 ISO 31000(2009)也提到考量要素有(1)社會、文化、政治、法律、道德、財務、技術、經濟及環境等層面 (2)組織未來目標及趨勢和對業務衝擊 (3)利害關係人的期望。針對公司各式營運活動或服務應區分優先順序及產品服務交付的緊迫性，才有辦法制訂公司 BCM 策略。

（二）第二階段：決定 BCM 選項

此階段，經查閱 BS 25999-1 並無詳細明確描述如何進行，但 BS 25999-1 內容亦提到營運持續管理為風險管理補充框架，在 ISO 27005:2008 Information Security Risk

management 就有明確定義當企業面臨風險的管理過程為(1)確定範圍(2)風險評估(3)開發風險處置計畫(4)風險接受(5)實施風險處置計畫(6)持續監控和評審風險(7)維持和改進風險管理過程，在 ISO 31000(2009)定義，風險評鑑(Risk Assessment)包含了風險識別(Risk Identification)、風險分析(Risk Analysis)、風別評估(Risk Evaluation)三個步驟。

1.風險識別(Risk Identification)

風險識別，主要目的是識別什麼事件或情況會導致業務遭受影響，在 ISO 27005:2008(2008)附錄 C 已經整理許多可能會造成 IT 中斷事件，如物理損壞(火災、水災…)、基礎服務失效(電源失效、通訊設備故障..)等皆有可能造成企業營運服務中斷。

2.風險分析(Risk Analysis)

藉由風險分析流程，來評估上述事件發生的機率及對企業造成損害程度，依據文獻「應用層級分級分析法建構金融業營運持續管理之營運衝擊關鍵要素」(賴俊吉 2008)論文參考，對金融產業最擔心是當災害發生時，造成最大衝擊為市場佔有率的流失。

3.風險評估(Risk Evaluation)

把預估的風險和組織的風險準則及預防措施比較，來決定風險的顯著性或剩餘風險。

4.風險處置(Risk Treatment)

面對剩餘風險在 ISO 27005(2008)提到可以採取四種風險因應措施(Risk treatment)：(1)減輕：透過各項措施，降低對組織的傷害(2)維持：經檢視各項控制措施，確認此風險是可接受範圍(3)規避:避免風險發生 (4)轉嫁：將風險轉嫁到第三方，如保險公司或廠商。因本研究主要著重於企業「異地備援」，故屬於採取「減輕」措施，故不另討論其他三種因應措施。

（三）第三階段：建置及發展 BCM 回應

1.企業持續營運計畫(BCP)制訂

天災的發生，總是存在不可預期性，所以企業持續營運計畫(BCP, Business Continuity Planning)制訂是非常重要的，在計畫中，可以明確表明什麼情況、條件啟動企業異地備援、每個人的工作及活動內容、及相關資源如何取得，在 BS 25999-1(2006)提到計畫內容應該包含(1)介紹(2)目的和範圍(3)角色與責任(4)計畫如何啟動(5)文件所有人及維持人員(6)具體的聯係方式(7)活動清單(如誰應該去那、如何去、在那集合..)(8)資源需求(如人員、基礎建設、技術設施、相關文件、供給及和利害關係人如何溝通)。

2.異地備援環境建置

本論文在 2.2 異地備援七種等級 章節已經提及七種異地備援等級，故不再多探討異地備援技術(如 IBM PPRC、IBM AIX LVM 等)或工具(如 Sysmantec BESR、VISION Double Take)，本論文主要還是從制度面進行探討，從「銀行資訊中心災害備援關鍵成功因素之研究」文獻(蔡登輝 2007)整理，可以確認異地備援環境建置的關鍵成功因素有下列(1) 主管支持(2) 充足預算(3) 明確的需求(4) 參與規劃的人員之技術能力(5) 備援方案之選擇(6) 專案管理(7) 相關部門配合度(8) 廠商技術能力 這八點，本論文也針

對上述八點請專家再次進行德爾菲法討論其重要性，除(5) 備援方案之選擇、(8) 廠商技術能力這兩點未取得共識外，餘專家都認為其餘六點是「異地備援環境」建置的關鍵成功因素。

3.異地備援環境例行性維護

災變是不可預期的，相信就算有良好的計畫、支出大量的預算來建置異地備援環境，然而，如果沒有事前準備、平時維護，當突然發生災變時侯，異地備援環境是否可以如預期般對外服務，我們從 BS 25999(2006)、金管局 本國銀行業務別檢查手冊(資訊)、金融控股公司檢查手冊-資訊作業(2001)、行政院研考會行政機關營運持續管理評估標準(2008)都有要求設備要定期保養並保留保養紀錄 、通聯方式、系統復原程序(SOP)、重要電子檔及相關文件有無異地存放等，相信只有平時有效準備，才能面臨真正突發的意外。

（四）第四階段：驗證、維護及自我評估

1.異地備援環境驗證

相信如何驗證「異地備援環境」之可用性，最好方式，莫過於將正式環境交易實際切換至「異地備援環境」實際運作，然很可惜，在台灣金融產業只有少數公司真正有辦法做到，而且在切換過程仍然存在對公司營運可能所造成風險及衝擊，所以在台灣金融產業，多數公司選擇驗證方式最好莫過於定期演練、藉由演練來驗證「異地備援環境」有效性。經由「銀行資訊中心災害備援關鍵成功因素之研究」(蔡登輝 2007)論文調查 18 家銀行統計，台灣銀行業多數會半年執行異地備援演練乙次，80%演練結果可以符合 BCP 預期的結果。

2.維護及自我評估

演練後的結果，除了可以明確發現不足地方，還可以提昇公司人員對災變的應變能力，在「以戴明循環檢視企業難備援建置以銀行業為例」論文(周士琛 2009)提到，每次演練結果可以成為(1) 定期演練為災害備援計畫的資料回饋機制(2)備援計畫的知識庫建立，另在 BS 25999-1 亦提出，演練結束後，組織應依據組織規模定期審視 BCP，配合組織目標、方針、環境等改變予以修正，當然組織亦可利用內部及外部稽核方式，協助組織 BCP 各項文件、環境等是否有確實進行維護及自我評估，在 ISO 27001(2005)則是強調採用”規劃-執行-檢查-行動(Plan-Do-Check-Act)”過程模型，適用建置所有 ISMS 過程，而「異地備援」則屬於在 ISMS 的其中一個部份。

參、研究架構與方法

一、研究架構

本研究架構基礎是參考 BS 25999-1(2006)整合風險管理(ISO 31000 2009)及戴明環理論(周士琛 2009;ISO 27001 2005;林金宏 2008)，透過各式文獻初步擬定「異地備援」建置程序及成功因素，以李克特五點量表設計問卷及前測，並運用德爾菲研究方法，取得專家共識，制定「異地備援」PDCA 各週期之所需檢核項目，最後，再以這些項目探索

九家金融機構執行現況，除了可以檢測項目的必要性，亦可瞭解各金融機構「異地備援」機制執行現況。

二、研究方法

本研究採用主要研究方法為下列二種，第一透過「德爾菲法」，取得專家對於「異地備援」生命週期所需之檢核項目，第二是以「個案驗證」方法來針對台灣金融產業之公司進行瞭解及分析並驗證透過「德爾菲法」取得之檢核項目之有效性。

（一）德爾菲法

德爾菲法(Delphi Method)是一種用於群體決策上的一種方法，是一種利用直覺判斷的預測術，多應用於「質性」研究。其主要目的，針對某個特定議題，借重各位專家經驗與知識，經過數個回合重覆、反覆回饋，取得專家一致性意見，以避免集體討論存在的屈從於權威或盲目服從多數的缺陷。本研究期藉透過德爾菲法及專家寶貴知識與經驗，得到建置「異地備援」生命週期各階段檢核項目。

（二）個案驗證

個案研究法適合以「組織」做為研究對象，適合於以實務面為基礎的問題進行研究，透過文件彙集、深度訪談等方法進行瞭解研究對象所存在之問題並予分析。然本研究檢核項目擬訂已參考台灣金融、傳產等產業之公司如何進行「異地備援」規劃及建置等工作。並期利用透過德爾菲法產生之「異地備援」生命週期各階段檢核項目，並抽驗部份金融產業之公司「異地備援」之現況，以期瞭解及分析，最後給予建議。

二、研究設計

（一）問卷內容設計

本研究問卷區分兩階段，第一階段採半開放式架構設計，首先透過第二章文獻探討(國際標準、論文…)及與部份專家先行訪談，初步擬定「瞭解組織和組織環境（內部及外部)」等七個階段共計 59 個檢核項目來分別探討，每個項目對「異地備援」機制的重要性，受訪者，除了可以針對這 59 個項目之必要性進行評分，如果發現這 59 個項目不足代表「異地備援」機制，亦可提供寶貴意見增加或修正裡面內容；第二階段採封閉式問卷，利用第一階段取得檢核項目，驗證及瞭解台灣金融產業「異地備援」執行現況。

（二）研究調查實施

研究調查區分兩階段，第一階段研究調查對象為於金融產業服務或服務於金融產業之廠商有一定工作年資且對於「異地備援」建置有一定經驗之專家人員進行問卷訪談及調查，問卷發送方式採電子郵件或由研究人員直接與受訪者面對面訪談方式之進行；第二階段研究調查對象為台灣金融產業之銀行、保險、證券等公司，以電子郵件方式寄送，以期瞭解及驗證上述公司「異地備援」現況。

（三）第一階段：德爾菲法進行及檢核項目之篩選

本研究問卷採用李克特五點量表，由受訪者依自己主觀看法，勾選適合的選項，如受訪者發現項目有不足地方，或問題、語意有不夠清楚，受訪者可於問卷「新增或修改項目」欄位加註意見及增修檢核項目內容，第一次問卷回收結束後，將針對受訪者意見，進行統計分析及依據每位受訪者回饋內容及意見，再次修改檢核項目及設計第二次問卷內容，並於第二次問卷內容將第一次結果回饋給每位專家知悉，俟第二次問卷回收結束

後，並開始進行項目篩選之工作，檢核項目篩選原則擬依 Chang(2002)等多位學者提出之標準，項目必須 CV≦0.5(表示專家意見為高度一致或在可接受範圍內)且「重要性」平均數≧4(受訪者意見為同意或非常同意)。

（四）第二階段：驗證及瞭解台灣金融產業「異地備援」執行現況

最後，本研究會依據德爾菲法所篩選出來的檢核項目，針對九家金融產業驗證及瞭解該組織現行「異地備援」機制執行現況，除了可以確認檢核項目的必要性外，亦可瞭解台灣金融產業「異地備援」執行現況，並給予統計、分析及建議。

肆、資料分析與討論

本研究內容主要區分兩大階段，第一階段，透過德爾菲法，取得「異地備援」機制的七個階段在 PDCA 四個週期所需的檢核項目;第二階段，利用德爾菲法取得的項目驗證現行台灣金融產業「異地備援」機制實施現況，並給予統計、分析並給予建議。

一、第一階段：透過德爾菲法取得檢核項

第一階段之專家成員的組成，擬請於金融產業服務計有部門主管等十人或服務於金融產業之廠商之二員資深工程師等人，上述人員皆有一定工作年資且對於「異地備援」建置亦一定經驗之人員進行問卷訪談及調查，並透過第一次及第二次德爾菲法回收資料並區分七個階段進行統計分析，經回收問卷結果，除 5 個檢核項目：1.參考社會文化環境 2.評估發生可能災變事件及機率 3.廠商的選擇 4.備援(份)工具或方案的選擇 5.備援地點的選擇 等項目無取得專家共識(CV≧0.5)，餘 44 個檢核項目均取得「有共識」(0.3≦CV≦0.5)或「極度共識」(CV≦0.3)且上述 44 個檢核項目平均數≧4(受訪者意見為同意或非常同意)，經比較第一次及第二次問卷結果，可以很明顯發現多數檢核項目的變異數均有縮小現象(表示專家認同度集中)，針對上述未取得專家共識的五個項目，經問卷回數結束後，根據資料分析及與部份專家訪談，得到下列結果：1.參考社會文化環境：雖在 ISO 31000 風險管理提到應將「社會文化」當作風險管理模型輸入變數，然在第一次問卷結果，已經多數專家認為該項目對於「異地備援」機制並非主要考量因為（第一次平均數 3.31、第二次平均數 3.23)，且也不明白為何「異地備援」機制與「社會文化」有關連，故該項目，因無法取得專家共識，且該項目權重(平均數<4，認同程度為：普通)，故本研究將捨棄該項目。2.評估發生可能災變事件及機率：在第一次與第二次問卷結果，均未取得專家共識（第一次變異數 0.86、第二次變異數 0.77)，經詢問專家意見表示，雖 ISO 27005 有列多種對資訊系統造成災變因素，但資訊系統持續營運，基本只要考量對企業造成最大衝擊事件即可（如機房火災、921 大地震)，無須每個事件都評估，否則將過度浪費人力成本，故本研究將捨棄該項目。在 3.廠商的選擇、4.備援(份)工具或方案的選擇　檢核項目：從資料可以發現，回答專家如為系統管理人員或廠商，多數對於這兩個項目都極為重視，但如為使用者端或安控人員等平常工作未與「異地備援」建置有直接關係者，多數都認為較不重要，從研究數據，本研究可以推論最主要原因為後端使用者直覺認為「異地備援」建置為系統管理人員工作，而廠商為輔助人員；反之，對於系統管理人員因直接面對「異地備援環境」建置工作，以經驗來說，如果沒

有好的「備援（份）工具」或「協助廠商」,「異地備援」環境建置是困難的。因兩端專家背景不同，才會導致此認知差異，相信再多做解釋及問卷調查亦無意義，故本研究將捨棄上述兩項檢核項目。5.備援地點的選擇：為第一次問卷回收之專家建議應增加該檢核項目，然在第二次問卷結果，很明顯未取得多數專家之共識（變異數 0.64），且部份專家亦反應，該項目應該是包含風險評鑑中的「明確定義災變發生後造成的衝擊程度」項目中，無須新增該項目，故本研究將捨棄該項目。最後，本研究從第一次問卷的 59 個檢核項目轉變至第二次問卷的 49 個檢核項目，再經捨棄 5 個項目後，得到「異地備援」七個階段在 PDCA 四個週期的關鍵 44 個檢核項目(如表 4-1)。

表 4-1 第二階段德爾菲法取得檢核項目

階段	檢核項目	變異數
瞭解組織和組織環境（內部及外部）	符合政府法令、法規及合同義務的要求	0.00
	符合公司政策、組織、文化、業務戰略目標、策略和方針	0.08
	符合公司資訊安全方針	0.14
	瞭解利害關係者(Stakeholders)的期望	0.27
	參考社會文化環境	0.53（刪除）
	符合公司營運持續計畫(BCP)	0.08
	符合公司風險管理計畫	0.08
進行風險評鑑	明確定義資產價值	0.44
	評估發生可能災變事件及機率	0.77（刪除）
	明確定義災變發生後造成的衝擊程度	0.31
	設定異地備援設備建置優先順序	0.08
	剩餘風險可被利害關係者(Stakeholders)接受	0.26
異地備援環境建置	參與規劃的人員之技術能力	0.19
	利害關係者(Stakeholders)參與異地備援規劃	0.17
	高階長官支持	0.14
	利害關係者(Stakeholders)支持	0.44
	成立專案組織	0.27
	指派專職部門或具有資歷人員負責異地備援規劃及建置	0.27
	相關部門配合度	0.14
	獲得充足資源(資金、人力、時間)	0.23
	資源衝突可得到有效溝通協調	0.27
	廠商的選擇	0.86（刪除）
	備援(份)工具或方案的選擇	0.53（刪除）
	備援地點的選擇	0.64（刪除）
異地備援計畫制訂	異地備援計畫文件化，並由高階管理層階簽署	0.40
	明確定義當災變發生，在什麼情況下，要決定啟動異地備援機	0.14

	制	
	明確定義當災變發生，何人可決定啟動異地備援	0.23
	異地備援計畫包含事故管理小組(IMT)來專門處理人員傷亡及傷害評估	0.23
	明確定義 RTO 及 RPO	0.14
	明確定義當災變發生，組織(不僅 IT 部門)內、外部各方的角色和職責	0.26
	當人員發生傷亡時，有無取代人力	0.23
異地備援環境例行性維護	系統程式，原始程式及目的程式、長期保留或重要之電子檔案異地存放	0.26
	通聯名單(例如:關鍵及替代人員及廠商)異地存放	0.42
	資訊系統復原 SOP、重要程式文件、清冊、密碼單等與相關系統文件異地存放	0.23
	資訊設備例行性維護及保養	0.08
	委外或供應商合約內容檢視	0.19
異地備援演練驗證	定期演練	0.19
	資訊系統標準復原程序手冊	0.26
	參與人員熟練程度	0.26
	廠商支援程度	0.42
	使用者納入演練測試	0.23
	每次演練採用不同腳本或模擬不同災變損失	0.23
	演練過程及缺失詳盡記錄	0.26
監控及持續改善	演練結果讓利害關係者(Stakeholders)知悉	0.31
	演練缺失及未達到指標(RTO/RPO)進行檢討	0.27
	專責稽核單位針對演練缺失改善情形進行追蹤	0.42
	演練缺失納入下期演練測試	0.19
	異地備援建立定期評審機制,及各式檔隨環境變化更新	0.27
	供應商合約內容隨著公司需求變更而調整	0.23

二、第二階段：驗證台灣金融產業「異地備援」執行現況

第二次階段問卷，主要目的為驗證台灣金融產業「異地備援」執行現況，本次計有九家金融公司（銀行:6 家;人壽:1 家;證券:1 家）協助本研究調查，調查方式為該公司提供一套有執行異地備援的資訊系統實施分析。

本研究問卷設計共區分三大部份，第一部份「基本資料」，主要是填寫受測者任職公司及執行「異地備援」資訊系統等相關資訊，以期瞭解「異地備援」執行完善程度是否和公司規模、公司類型、維運人數等是否有對應關係；第二部份「異地備援機制檢核」，主要利用第一階段透過德爾菲法取得 44 項檢核項目來評量該公司資訊系統「異地備援」機制的完善程度；第三部份「受測者自評」，目的為瞭解受測者對於第二部份所評鑑之資訊系統「異地備援」機制滿意程度並驗證是否和第一階段專家看法是否一致。第二部份「異地備援機制檢核」評分方式為假設每個項目分數為 1 分，如該項目有區分層次(如

符合程度為「完全不符合」、「多數不符合」、「部份不符合」、「多數符合」、「完全符合」等五個選項，則依比例 0、0.25、0.5、0.75、1 給分)，經統計結果，九家公司得分如表 4-2

表 4-2 第二次階段-九家銀行檢核項目符合程度

A	B	C	D	E	F	G	H	I
41.85	9.5	38.35	36.75	36.25	39.05	27.5	29.95	36.3

（一）第二階段問卷資料分析

透過現行九家台灣金融產業公司問卷回饋進行驗證，本研究有部份發現事項：

1.「異地備援」是否能降低公司面對重大災害之衝擊?

從第二階段問卷回饋資料，可以明顯發現，原本九家公司在不考量異地備援情況，如發生日本 311 大地震或泰國大水患時，對七家公司衝擊程度為「極度嚴重」，兩家公司為「嚴重」等級，如果有建置「異地備援」機制，當發生重大災害事件，很明顯降低了對公司的衝擊程度（極度嚴重：1、嚴重：1、尚可：3、很小：1、非常小：3)。

2.「異地備援」能否滿足資訊系統必須對外服務時間?

資訊系統恢復時間長短，與支出成本多少有絕對關係，任何公司不可能針對所有資訊系統都以無上限成本來做到「層級 6：零資料遺失」層級，所以必須在「業務衝擊」和「成本」取得一個平衡，經統計結果，有 78%要求當資訊系統毀損，必須於四小時內完成修復，並對外營運，然多數公司亦表示以現行異地備援機制如面對像日本 311 大地震或泰國大水患時，有 56%認為可以符合「異地備援計畫」所要求的系統回復時間（Recover Time Objective , RTO）時間、22%認為會有些許落差，僅 22%認為會與「異地備援計畫」所要求的系統回復時間（Recover Time Objective, RTO）時間落差很大及完全無法評估，從此可以推論，台灣金融產業之公司當發生重大災難事件，如果有良好的「異地備援」機制，將可以減少災後資訊系統復原時間。

3.「異地備援」能否滿足公司最大忍受資料遺失時間?

如前所言，「異地備援」必須在「業務衝擊」和「成本」取得一個平衡，故不可能要求每套資訊系統都做到「零資料遺失」層級，從調查發現 89%以上金融公司最多可以容忍四個小時資料遺失，然多數公司，認為在面對像日本 311 大地震或泰國大水患時，有 78%都能符合「異地備援計畫」所要求的資料誤差時間（Recovery Point Objective , RPO）或誤差很小，僅 22%時間落差很大及完全無法評估，從此可以推論，台灣金融產業之公司，當發生重大災難事件，如果有良好的「異地備援」機制，可以減少資料遺失筆數。

4.取得資安認證能有效協助「異地備援」機制建立?

本次協助受測公司之資訊系統，計有七間取得 ISO 27001/BS 5599，其中一間公司之資訊系統亦通過 BS 25999 之認證，僅有兩間公司未取得資安相關認證，從表 4-3 很明顯顯示有取得資安認證在「異地備援」符合項目數較高。

表 4-3 資安認證與異地備援機制分析

取得證照	公司	符合項目數	平均值
取得 ISO 27001/BS 5599 及 BS 25999	I	36.3	36.3
只取得 ISO 27001	A	41.85	37.03
	F	39.05	
	C	38.35	
	D	36.75	
	E	36.25	
	H	29.95	
無取得資安相關認證	G	27.5	18.5
	B	9.5	

5.使用者滿意程度與符合檢核項目數對應關係?

經與受測人員對該公司之資訊系統的「異地備援」機制的滿意程度進行比較，從表 4-4 明顯看出，受測人員對於該公司之資訊系統的「異地備援」機制的滿意度程度越高，所符合檢核項目就較多，可以推論專家看法和受測人員看法為一致的，再此驗證所取得檢核項目的有效性。

表 4-4 檢核項目和滿意程度關連分析

等級	公司	分數
非常滿意		
滿意	A	41.85
滿意	F	39.05
滿意	C	38.35
滿意	D	36.75
滿意	I	36.3
滿意	E	36.25
滿意	H	29.95
普通	G	27.5
不滿意	B	9.5
非常不滿意		

6.「異地備援」機制最差的五個項目

經統計及排序受測公司「異地備援」44 個檢核項目，發現這九間公司執行最差的五個項目分別為(1) 供應商合約內容隨著公司需求變更而調整(2)成立專案組織(3) 異地備援計畫包含事故管理小組(IMT)來專門處理人員傷亡及傷害評估(4) 定期演練(5) 使用者納入演練測試，相關說明及本研究討論說明如下：

(1)供應商合約內容隨著公司需求變更而調整

藉由受測者回饋資料發現，多數「異地備援」與供應商的合約，不會因為公司組織或「異地備援環境」變動、風險管理、持續營運計畫改變等因素，立即與供應商修改相關服務內容，大多都是等到與供應商合約到期(有些公司是一年一簽，也有部份合約週期超過一年以上，甚至有公司從未調整與供應商合約內容)後才調整服務內容，這也曝露一個風險，當「異地備援環境」等因素變更，現行與供應商的合約是否仍滿足「異地備援計畫」所要求的水準。

（2）成立專案組織

成立專案組織有時對專案進行是種幫助，但相對亦會增加額外的負荷(因為參與人員越多，溝通、協調的工作就越複雜)，「高階主管的支持」(平均分:0.74)及「獲得充足資源(資金、人力、時間)」(平均分:0.75)比對「成立專案組織」(平均分:0.5)對「異地備援環境建置」幫助程度較高。

(3)異地備援計畫包含事故管理小組(IMT)來專門處理人員傷亡及傷害評估

藉由受測者回饋資料發現，多數「異地備援計畫」均未包含事故管理小組(IMT)成員，姑且不談像日本 311 大地震如此重大天災，如發生像 921 大地震或大樓火災時，人員傷亡、設備毀損評估究竟由誰來做？相信多數「異地備援計畫」都會撰寫由某位高階主管決定啟動「異地備援」機制，但多數都是指單一系統毀損的狀況下，如果當同時間多數資訊系統皆毀損、部份人員發生傷亡事件，豈是一名高階主管有辦法短時間評估及做決策?此時應該要有事故管理小組(IMT)來執行人員傷亡及損害評估。

(4)定期演練

藉由受測者回饋資料發現，多數「異地備援演練」次數，為一年乙次，雖符合 BS 25999 的標準，但相信「異地備援演練驗證」階段完善程度與系統是否能符合預期時間對外營運是有對應關係，且演練期間才更容易發現到現行「異地備援」機制許多問題，以利後續改善現行機制的不足及缺陷。

(5)使用者納入演練測試

藉由受測者回饋資料發現，多數「異地備援演練」參與人員大多僅挑少數（或代表性）來參演，從這裡可以思考兩個問題，第一、當災變發生時，業務單位是否能無感就切換到「異地備援環境」執行正式環境交易?且執行交易內容是否能全部和正式環境所提供的服務相同，如果不是，當災變發生時，業務單位是否會發生手忙腳亂，不知所措情形? 「異地備援演練」有時不該只考量資訊部門或資訊系統能否復原即可，應該從業務角度去思考。第二、異地備援資訊系統及週遭軟硬體環境效能是否和正式環境相同?因為並沒有試過全部業務單位同時執行交易，且如果遇到交易峰時情況，現行的「異地備援環境」效能能否負荷?故在 BS 25999 才會提到，至少要有乙次或一年以上的週期進行全面或大規模演練。

伍、結論

一、藉由「資安認證」取得，以強化公司「異地備援」機制

從第四章研究發現，取得資安認證（BS 25999、ISO 27001）公司，在「異地備援」符合之檢核項目的確高於未取得認證公司，而且可以藉由第三方稽核力量（如 BSI），以他們寶貴的經驗來協助公司檢視那些不足需要改進的地方，而且相信當公司取得這些資安認證，也更有說服力，增加您的使用者對該公司資安信心，以提升業務行銷能力。

二、「異地備援」不該只是公司資訊部門工作

在第四章研究發現，「異地備援演練」階段，參與單位，只有少數業務單位會參與，主要原因為業務單位總是關心，什麼方式可以提高效率、降低成本、增加獲利，而公司資訊部門就是提供及維運這些工具的組織，多數的業務部門會認為資訊系統「異地備援」，應該要由公司資訊部門全權負責，但不論在 ISO 31000、BS 25999 都持續提倡利害關係人的觀念，IT 永遠是公司的後勤部門、是業務的推手，不論在持續營運管理(BCM)或風險管理，都應該落在公司高階主管或相關部門權責上，而不該僅由 IT 部門負責。風險管理的目的，不單單只是一昧的規避風險，而是如何運用公司的有限資源下，將風險及對公司的損害降至最低。而 IT 部門是無法進行風險管理，因為他的資源來自各業務部門，他的風險的面對，也來自各業務部門可承受多大的外在壓力及損失。ISO 20000 或 ITIL 制度的導入，相信可以讓業務部門與 IT 組織更緊密的結合。

三、有效管理企業整體「異地備援」機制並利用本研究所產出檢核表檢視及評量

「異地備援」機制非僅於「異地備援環境建置」階段，而是如何有效管理及持續維運此機制，當企業準備導入「異地備援」時，企業應由管理階層指派一人或多人來管理整體「異地備援」機制，並建立「異地備援」推動小組，藉以制訂相關規劃、計劃等文件及明確定義所屬人員職責，並由稽核小組人員定期檢視及評量該公司資訊系統「異地備援」機制完善程度。本研究經由第一階段取得「異地備援」PDCA 的四個週期 44 項檢核項目，並於第二階段個案驗證，已可確認本檢核表之有效性。故期爾後企業如有任一資訊系統要導入「異地備援」，可由「異地備援」稽核小組或專案品管人員利用本研究所產出之檢核表來檢視及評量該系統是否符合「第一階段：瞭解組織和組織環境」至「第七階段：監控及持續改善」各階段應注意事項及需完成之步驟，例如：企業稽核人員利用每年定期查核時，可利用本檢核表，檢查資訊系統「異地備援」建置，有無符合企業制定之「營運持續計畫」、「風險管理計畫」；專案品管人員，審視資訊系統「異地備援」功能之建置時，可利用本檢核表確認是否有先完成「營運衝擊分析」步驟。

四、週期性的演練及環境切換，來檢驗「異地備援」環境運作

不可否認，所有「異地備援」機制的維運工作，只有在演練及真實切換至異地環境才能真正顯現出現有的不足及缺陷地方，再配合不同「演練情境」及稽核或高階主管的缺失追蹤，才能將「異地備援」的完善程度發揮至最高，在本研究第四章案例，發現 A 公司的「異地備援」機制符合的項目數為 41.85，幾乎和滿分 44 項目相距不遠，本研究覺得最大差異原因是該公司一年超過二次以上演練為主要原因，這也是該公司與另外八間公司的最大不同之處。

參考文獻

1. GB/T 20988—2007 資訊系統災難恢復規範，2007，中華人民共和國國家標準。
2. 行政院及所屬各機關資訊安全管理規範，1999，行政院研考會。
3. 何星翰、呂敏誠，2010，『由資訊安全管理之風險評鑑協助企業營運永續確保核心競爭力』，品質月刊。
4. 吳佳翰、溫紹群、黃永婷，2011，『資訊風險管理大躍進－臺灣土地銀行資訊風險管理經驗交流』，勤業眾信 企業風險管理服務季刊。
5. 周士琛，2009，以戴明循環檢視企業災難備援建置以銀行業為例，國立台灣科技大學 管理學院。
6. 風險管理及危機處理作業手冊，2009，行政院研究發展考核委員會。
7. 陳明玉、蔣經華，2008，『BIA 在企業營運持續管理系統之應用』，2008 工業安全衛生技術輔導成果發表會。
8. 湯小芊，2009，『論銀行業業務連續性計劃 IT 保障』，FINACE & ECONOMY 金融經濟。
9. 資策會，2011，『臺灣行業別資訊應用現況與展望』，2011 資訊服務產業年鑑。
10. 蒲樹盛，2005，『營運持續管理 (BCM) 之國際標準及管理作為』，財金資訊雙月刊。
11. 蒲樹盛，2006，『政府部間營運持續管理(BCM)國際指南介紹』，研考雙月刊。
12. 樊國楨、黃健誠、林樹國，2011，『資訊安全管理系統政策探微:根基-政府機關之異地備援個案』，前瞻科技與管理。
13. 蔡登輝，2007，銀行資訊中心災害備援關鍵成功因素之研究，世新大學資管所碩士論文。
14. 蔡耀宗，2007，『企業之事業繼續經營(BCM)』，品質月刊。
15. 賴俊吉，2008，應用層級分級分析法建構金融業營運持續管理之營運衝擊關鍵要素，碩士論文，國立臺北科技大學。
16. 蘇建源、蔡旼修、阮金聲， 2011，『以個案分析法探討金融業之企業營運持續管理』，電腦稽核期刊 24 期。
17. Business Continuity Institute (BCI), “Publicly Available Specification 56(PAS 56)”, PAS 56, 2003.
18. IBM Redbooks, “Disaster Recovery Strategies with Tivoli Storage Management”, 2002.
19. ISO 27001. “ISO 27001 Information Security Management Standard”, International Standard Organization, 2005.
20. ISO 27005. “ISO 27005:2008 Information security risk management”, ISO, 2008.
21. ISO 31000. “ISO 31000 Risk management — Principles and guidelines”, ISO , 2009.
22. Technical Committee BCM/1. “BS 25999-1 Code of practice for business continuity management”, British Standards Insitute, 2006.
23. Technical Committee BCM/1. “BS 25999-2 Business continuity management — Part 2: Specification”, British Standards Insitute, 2007.

Construction of Taiwan's financial industry "Disaster Recovery"

PDCA checklist

Dr. Ruey-Shiang Shaw
Department of Information Management Tamkang University
rsshaw@mail.tku.edu.tw

Author
Taipei Chengshin University of Science and Technology
james@mail.tku.edu.tw

Jen-chen Lai
Department of Information Management Tamkang University
799630107@s99.tku.edu.tw

Abstract

Lessons from the Disaster of East Japan Great Earthquake and Tsunami 311 reflect that Taiwan is a country with frequent earthquakes. The quality of Disaster Recovery of information system of finance industries is concerned about enterprise profit and business continuity. But for their customers, that is more important than bank profit and business continuity because it is related to customer's property.

With the collected over literature, relative study and discussion with experts, this research gets 44 Check items by Delphi method in seven stages of Deming Cycle for Disaster Recovery of information system of the finance industries.

Use these 44 check items to verify the status quo of Disaster Recovery implemented in the nine financial companies and make sure of their validity and necessities. Suggestions are offered following the analysis of reply data from nine financial companies.

Keywords: BCM, Disaster Recovery, PDCA, ISO 31000, Delphi Method