聯徵中心「災害復原機制」之介紹

吳嘉川／金融聯合徵信中心資訊部

一、前言

資訊科技治理（Information Technology Governance）的議題近來在國內外愈來愈受到重視，牽涉的內容包含了風險管理、資訊安全、成本效益、營運持續、法規遵循等範疇，而對於一個企業而言，其最終目標不外乎是實現企業的永續經營，基於企業對永續經營理念的重視，災害復原的觀念也因而被企業所重視。災害復原的目的是為了在發生天災、人為疏失或惡意破壞造成資訊系統損害時，能以災害復原機制快速回復至企業正常或可接受的營運水準，以確保企業的永續經營。除了災害復原機制的建立，更重要的是需有完整的災害復原計畫，及持續的維護、管理與演練，以確保備援機制的有效性。

聯徵中心對於災害復原的重視起源於1999年9月台灣921大地震，及2000年5月汐止東方科學園區大火兩個重大意外事件的發生，經過一連串縝密的籌劃，在2001年9月已開始建置第一代的異地備援中心，同一個月內相繼發生了美國雙子星大樓的恐怖攻擊事件，及台灣納利颱風造成的台北大淹水兩大災害，更確立了異地備援中心的重要性。為了讓備援機制更臻完善，於2005年2月著手建置同地熱備援機制，以防重要的核心系統因單一電腦設備故障造成的營運中斷；同年12月，於同地熱備援中心建置完成後，開始建置更高水準的第二代異地備援中心。

二、目前聯徵中心災害復原機制介紹

(一) 同地熱備援機制

此處所稱「同地」指的是位於同一個辦公場所；「熱備援」指的是相關的備援電腦設備、作業系統、應用系統、網路設備等，是處於啓動狀態，可於數秒或數分鐘內，自動或手動啓動備援機制。備援系統可能是以負載平衡的方式運作中，或以待命的方式隨時準備接管運作，視系統及應用程式之架構而定。同地熱備援建置之目的是為防止單一電腦設備損壞造成對外服務之中斷。

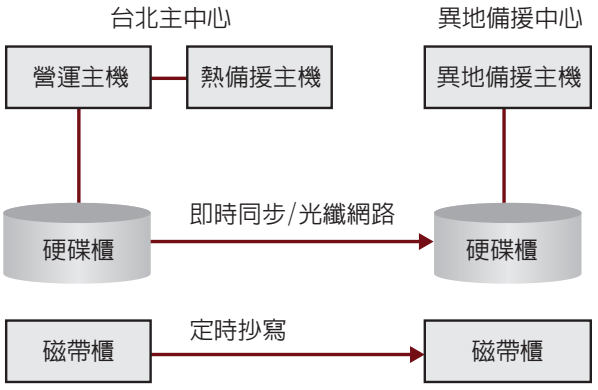
1. **目標**：達成重要核心系統之即時備援及切換。
2. **範圍**：聯徵中心對外營運之網際網路查詢、伺服器連線查詢系統，包含所使用之相關作業系統、應用程式及資料庫。
3. **架構**：簡易備援架構圖請見圖一。

(二) 異地備援機制

此處所稱「異地」指的是位於不同辦公地點；相關的備援電腦設備、作業系統、應用系統、網路設備等，是處於待命狀態，可於1至2個小時內，以手動方式啓動備援系統。備援系統平時處於待命的狀態，於災害發生時依權責主管命令啓動備援系統。異地備援建置之目的是，當意外災害造成整個資訊中心服務之中斷時，可於短時間內回復至特定的服務水準。

1. **目標**：達成重要核心系統之異地備援。回復時間目標(Recovery Time Objective, RTO)為系統切換2小時、對外營運4小時內完成；資料回復點目標(Recovery Point Objective, RPO)為主中心已完成的交易資料皆會同步到異地備援中心。
2. **範圍**：包含聯徵中心對外營運之三種信用資料查詢系統：網際網路查詢、伺服器連線查詢、檔案傳輸查詢及所使用之作業系統、應用程式及資料庫。另外，還涵蓋了資料倉儲資料庫、主機資料維護及大型磁帶館之備份資料。
3. **架構**：簡易備援架構圖請見圖一。

圖一　簡易備援架構圖



(三) 資料備援機制

除了上述兩種系統面的備援機制外，針對重要的資料及程式，聯徵中心尚有一套離線媒體的備份與管理機制，主要內容包含：

1. 備份磁帶第三地儲存：將資料庫、重要程式或資料之備份磁帶，儲存至主、異地中心之外的第三地媒體儲存地點。
2. 磁帶讀取測試：定期讀取磁帶資料，以確認磁帶之可用性。
3. 定期淘汰舊磁帶：定期汰換超過使用年限的磁帶，以防磁帶因老舊而毀損。

三、災害復原計畫 (Disaster Recovery Plan, DRP）

為了使備援機制能長久有效運作，聯徵中心訂定有備援演練計畫，並每年進行異地備援切換演練，除了動員內部各部門參與演練，同時也函請各金融機構熱烈參與，以驗證異地備援機制之有效性。

(一) 演練計畫應注意的重點

1. 演練範圍的界定

定義本次演練涵蓋的資訊系統、網路、作業項目、對內及對外服務等。

2. 演練情境的設計

演練計畫內應預先設計好不同的情境或劇本（Scenario），以符合實際上可能發生的各種狀況。

3. 演練之目標

設定演練的回復時間目標（RTO）、資料回復點目標（RPO），或有其他設定要達成的目標。

4. 時程之規劃

事先規劃好各項作業時程，以協調各部門參與人員、外部參與人員及支援廠商的時間。

5. 參與的部門

規劃好需要參與演練的部門、人員及其作業項目與程序。

6. 參與的外部機構

事先通知需參與的外部機構，及其需配合的作業事項，避免影響外部機構的日常作業。

7. 支援的廠商

協調系統或網路維護廠商，以防演練中設備異常造成額外的風險。

8. 動員的方式

訂定人員、車輛的動員方式，可依演練目標的不同，採集中動員或機動動員。

9. 標準作業手冊

相關的操作皆應建立標準作業手冊，以減少人為作業的失誤，且有職務異動時容易將技術轉移給其他人員。

10. 相關文件之審閱及更新

資訊系統、網路或作業環境會因時間而變動，相關的作業程序及手冊應隨之更新，才能維持操作的正確性。

11. 問題的追蹤與解決

演練過程中發生的異常問題應予紀錄、追蹤並解決之，以減少未來演練再發生同樣的問題。

12. 人員的配置與訓練

應事先規劃適當的人員並給予訓練，以促使執行作業的過程更為順暢。

13. 演練的頻率

規劃演練的執行頻率，以維持計畫的長期有效性，並符合相關國際標準的規範。

14. 演練之成效

可依目標達成程度、發生的問題及問題解決等項目，評估演練之成效。

15. 啓動程序

明訂啓動復原程序的管理層級及指揮程序，在災害發生時能發揮最即時的命令傳達。

16. 復原機制之維持

維持復原機制的有效性，應考慮系統、網

路、作業面的變更管理，並規劃人員的訓練與備援。

17. 相關管理標準的符合

考量計畫內容是否符合相關國際標準規範，如資訊安全管理標準ISO27001、資訊科技服務管理標準ISO20000等。

18. 與企業目標或計畫一致

檢視復原計畫是否與企業的整體目標或計畫一致。

(二) 聯徵中心歷年異地切換實際營運概況

2006年11月4日進行了專案驗收前的首次異地備援切換演練，共有43個會員機構參與；2007年11月25日進行第二次的年度切換演練，共計有31個會員機構參與；2008年12月20日進行第三次的年度切換演練，共有35個會員機構參與，歷年切換演練提供對外查詢服務及內部作業之目標皆順利達成。會員機構參與的概況請見表一：

表一　會員機構參與演練概況

舉辦日期	參與會員家數	會員查詢筆數	開放異地查詢時間
2006/11/04（六）	43	40260	11:00~16:00
2007/11/25（日）	31	6448	11:00~16:00
2008/12/20（六）	35	19450	11:00~16:00

(三) 持續改善事項

聯徵中心每年除了進行異地備援中心的實際營運切換演練外，更時時思考如何使備援的機制更加完善，目前正進行下列的改善措施：

1. 建立臨時的第三地對外作業中心

模擬於災害發生時，除了異地備援中心之外，另外建立臨時的對外作業中心提供服務，以更逼近實際狀況。

2. 增加Windows伺服器備援

考量增加支援內部作業的Windows系統備援，以縮短內部作業的回復時間。

3. 人員能力之備援

建立組織內部人員的備援機制，使得技術及經驗可以傳承。

四、災害復原之成功要素

災害復原機制應事先設想可能的情境，並規劃好應變的措施。定期執行演練可以驗證災害復原機制的有效性及人員應變的能力與熟悉度，並可檢視計畫的可執行度，進行必要的修訂。以下列出一些災害復原機制的成功要素，可作為一般企業建立災害復原機制的參考。

(一) 高階主管的重視

因高階主管基於對永續經營理念、風險管理的認知或相關法規的要求，重視資訊系統及業務的備援，災害復原機制才能有效建立。

(二) 充足的預算

災害復原包含了複雜的資訊系統，建置的成本依其備援的規模及等級而定，備援的範圍愈大、要求的回復時間愈短，則建置的成本愈大。若沒有足夠的預算，建置的品質可能因而下降，無法符合預期。

(三) 明確的需求與目標

依組織經營理念及策略，考量專案的成本效益，透過業務衝擊分析，評估可容許業務中斷的時間，據以確定專案的需求及目標。

(四) 專職的團隊

企業應成立一個專職的營運持續團隊，持續關注企業營運環境裡的運作風險，同時擬定一份管理程序，以防範在資訊科技被高度運用的時代，災害發生所帶來的衝擊也隨之擴大。營運持續牽涉了企業的業務流程及人員指揮管理的問題，非資訊人員有權力推動的。

(五) 人員的能力

復原機制包含了眾多的資訊系統、網路、應用程式運作，具有較高的技術複雜度，負責規劃、執行與管理復原機制的相關人員，需具備有整合的技術、對業務流程的熟悉及管理的能力，才能將整個專案規劃及管理的更加完善。

(六) 注重整體的規劃與管理

由於復原機制的複雜度高，應注重整體的規劃與管理，統合資訊技術、業務流程及人員管理等不同層面，才能將可能遭遇的問題降到最少。

(七) 專案管理之品質

復原專案建置的過程中會遇到各種問題，良好的專案管理品質可以有效的解決問題，而不是忽略問題。

(八) 相關部門之配合度

組織內每一位成員應對災害復原的重要性有正確的認知，才能由上而下規劃管理，由下而上落實執行。

(九) 人員的教育訓練

復原機制涵蓋了眾多的程序，對於執行的人員應定期實施教育訓練，使其操作更加熟練，能有效減少錯誤的發生，並縮短復原所需的時間。

(十) 廠商的技術能力

廠商需要具備有高度的技術整合能力，才能提出適當的基礎建設架構，並確保專案建置的品質。

(十一) 廠商的支援能力

由於業務、資訊系統或網路可能因時間而發生變動，影響了原來建置的復原機制，導致執行時發生各種預期外的狀況，此時若沒有廠商的技術支援，會導致復原時間大幅拉長，甚至有業務停頓的風險，尤其當復原機制的等級或逼真程度越高時，此種風險程度越高。

(十二) 作業程序的完整度

完整的作業程序能降低復原機制執行的難度、減少錯誤發生的可能及促進技術的傳承，

因此需要建立正確且完整的作業程序。

(十三) 持續的改善

由於復原機制中的各種程序可能因為時間變動而造成作業流程、資訊系統或網路等各種層面的變動，導致復原程序發生問題甚至失敗，因此需要持續對復原機制進行演練與維護，才能維持機制運作的長期有效性，並確保目標的達成。

五、相關的國際標準與發展趨勢

隨著資訊科技治理、企業營運持續等觀念越來越受重視，相關的國際標準也陸續出爐，提供企業參考或遵循的依據。

(一) 近年來相關的國際標準

1. ISO 27001:2005 資訊安全管理系統

2005年10月由國際標準組織（International Organization for Standardization, ISO）發佈的資訊安全管理標準。它是一套資訊安全管理的準則與規範，可以協助組織鑑別、管理和降低資訊資產所面臨的各種威脅與風險，確保資訊資產的機密性、完整性與可用性。

2. ISO 20000:2005 資訊科技服務管理

2005年12月由國際標準組織（ISO）發佈的資訊科技服務管理標準。它是一套具有共通性與實用性的資訊科技（Information Technology, IT）管理方法，能協助組織的IT流程與方法最佳化，並確保組織所提供的服務符合內、外部客戶之需求，及在有限的預算下，提升系統及服務的可靠性與可用性，並且符合國際標準規範。

3. BS 25999:2007 營運持續管理

2007年11月由英國標準局（British Standards Institution, BSI）發佈的企業營運持續管理規範BS 25999-2:2007。2006年12月發佈企業營運持續管理實務準則BS 25999-1:2006。它是一套具有共通性的管理標準與指導綱要，指導組織如何建立良好的防護機制，以確保營運持續能力，在全球化的競爭浪潮下，維繫組織的永續經營能力與卓越的競爭力。

(二) 災害復原發展趨勢

1. 災害復原概念之擴大

上述國際標準對於災害復原、營運持續計劃或營運持續管理都有相關的建議，復原概念也逐漸由資訊系統備援擴大至業務面的復原，甚至加入風險管理的概念，底下簡單說明相關的概念：

(1) 災害復原（Disaster Recovery, DR）

因應未來可能遭受的天然的或人為的重大災害，能迅速回復重要的營運資訊系統。

(2) 營運持續計劃（Business Continuity Plan, BCP）

除重要營運資訊系統外，將企業業務層面納入計畫，以維繫組織之長期運

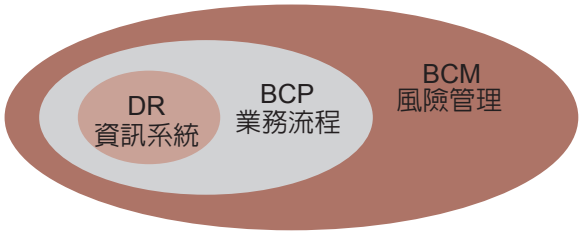
作。營運衝擊分析（Business Impact Analysis, BIA）是發展BCP的首要分析工作，將影響企業營運的威脅與衝擊依嚴重等級及緊急程度予以區分，以利後續回復計畫之訂定。

(3) 營運持續管理（Business Continuity Management, BCM）

提升企業長期競爭力，結合風險管理，以營運持續計劃為基礎，從建立、推行、運作、監督、檢討、維持至持續改善相關機制，以強化企業恢復力（Enterprise Resilience）。

(4) 災害復原（DR）、營運持續計劃（BCP）、營運持續管理（BCM）之相互關係請見圖二。

圖二　DR 關係圖



2. 人員備援概念之重視

人員是企業的重要資產，人員的技術與經驗傳承可以使企業運作更為穩定及順暢。目前的復原機制著重在資訊系統、復原計畫及復原程序，在風險管理的概念加入後，人員備援的概念也逐漸被重視，當主要業務負責人不在時，有其他人員可立即接手處理業務。

3. 重視資訊基礎建設（IT Infrastructure）

舊有的異質系統可能會使得復原機制之程序繁複、難以整合，若能注重資訊架構的整體規劃，適時採用新的技術標準，可使各種資訊系統容易界接與整合，也可簡化復原的程序，不過初期高額的置換成本則是不可避免的。

六、結語

隨著企業營運版圖及業務的擴大，企業對資訊化的依賴程度也日益加深，各種資訊系統不斷增加，造成系統的異質性、複雜度及網路連結的複雜性皆隨之增加，一但資訊系統遭受災害，將造成重大的金錢損失，甚至營運中斷，損失的商機與無形商譽更是難以估計。災害復原或營運持續管理應以企業未來遠景做整體性的考量，考量成本效益、可接受風險、最低營運水準等因素，視企業的需要建立合宜的復原機制，一但面臨重大災害時，必能降低企業損失，維繫企業的永續發展。