從《資訊風險管理》談《緊急應變計畫》（上）

－風險管理的規劃與執行-

壹、前言

98 年 1 月 7 日桃園機場入出境電腦的開年當機，即爲一例資訊風險管理失漏的殷鑑。

其實，風險管理本就存在我們平日生活中，其領域涵蓋各行業、個人與團體；生活上的投資、人壽保險、第三責任險、甚至於行舟走車的安全意識，都屬風險管理的一種類型，在專業領域部份，諸如：食品安全、藥品管理、環保、…等等，亦皆屬之；而資訊設備的持續運作祇是其中之一種。

因爲涉及人事時地物等各環境因素的不確定性變化，風險不可能完全避免，所以需要以管理爲手段，加強事前預防、事中因應、及事後回復的處理，期以降低風險發生的概率，達到零風險的趨近值；同時，在風險發生時，仍能維持最基本機能的營運，以減少財物損失和形象破損。此即謂深度風險防禦也。

一般而言，風險管理是以「避免」、「保護」，和「減緩」等三個階段構築而成，透過設計、建置、訓練、管制等時期去避免事故的發生；遇有異常時，則以備援、回復等手段去保護業務的不中斷運作；而在事故不幸發生時，則以最短時間重建或採替代方案維持最基本業務功能，減緩事故對組織業務的損害和影響。

無論政府單位或民營企業，時下的業務幾乎都依賴電腦處理，電腦系統涵括硬、軟體、網路、機電、空調等設施，一個環節出現問題，輕者局部停擺，重者全部業務癱瘓；兼之，服務人員和被服務者皆習慣於電腦作業，即使可以轉換成人工作業，雙方都無法暢快適應，效率更不用說了。

藉由風險管理，建構一套緊急應變計畫，是資訊管理的最終目標。

貳、最需風險管理的行業

以政府機關而言，凡與公共安全、社會秩序及人民權益相關者，如：警政、地政、關務、稅務、電力、石油、自來水、航管、捷運、交通號誌等 21 體系，及金融、證券、電信、製造、醫療等 5 大行業皆爲最必需加強風險管理的行業；而依其所屬機關之職司，擴大及於國營事業與民間者有台電體系、中油體系、醫療業、電信業、航管體系、儲匯體系、金融業、證券業、製造業、中小企業、流通業、財稅體系、關務體系、警政體系、地政體系、自來水體系、公路號誌體系、鐵路號誌體系、捷運體系等相關業者。詳如圖 1.

圖 1、最需風險管理的行業

參、風險成本的考量因素

依據 DATAPRO 研究，見圖 2，一般電腦中心當機 4 天，則單位業務活動力(activity)將下降 60%，而銀行則只須 2.5 天。

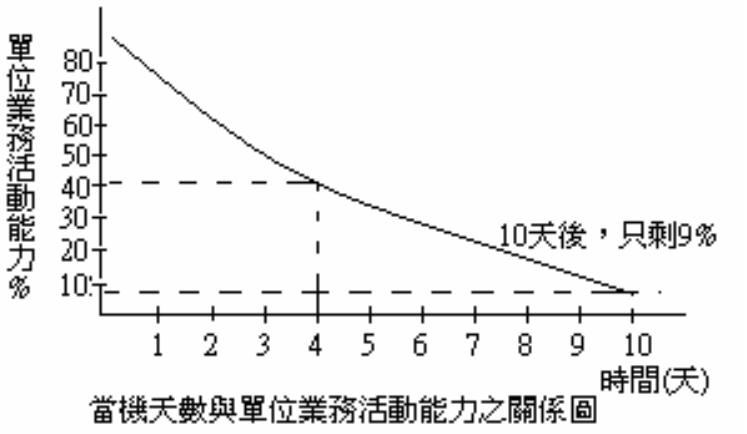

圖 2

也由於沒有百分之百的安全風險防範方法，所以風險保障的投資亦非毫無限制的投入；風險控制的投資是一 trade-off 衡量的課題，在可接受的當機時間與最經濟回復成本等兩者之間取得平衡點，以獲取最大效益。如圖 3：

(一) 可接受的當機時間越長，其回復成本越小；
(二) 但對於重要業務而言，可接受的當機時間越短，其回復成本雖然越高，但其衝擊損失較少。
(三) 是以，亦可經由可接受的回復成本和可接受的衝擊損失，來決定理論上的可接受的當機時間。

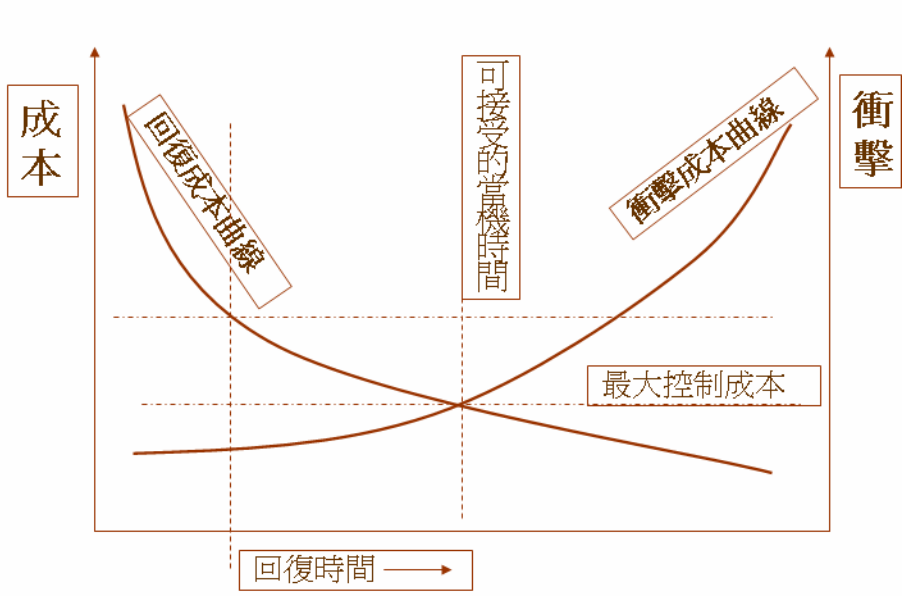

圖 3、可接受的當機時間與最經濟回復成本

是以，風險安全保障的課題必需考量業務的重要性、衝擊損害程度、可容忍的回復時間（可接受的當機時間）、回復成本等諸項因素，擬妥各項業務的緊急因應對策。

肆、風險管理的步驟

風險管理的步驟分爲三階段：風險確認、風險評估、風險控制。如圖 4。

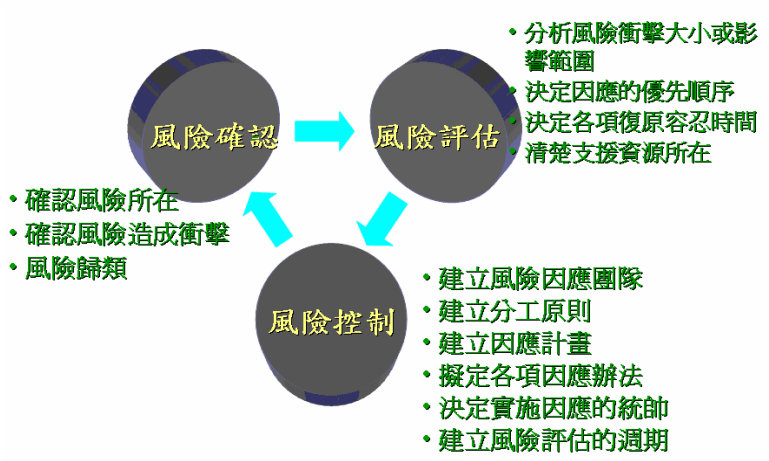

圖 4、風險管理的步驟

亦即，(一)經由風險確認找出資訊業務潛藏的風險所在，及造成風險的危害性因子的現行防禦作爲；其次(二)透過勾風險評估以分析各項業務的風險衝擊大小或影響範圍，和綜合各項業務中斷所能容忍的時間考量，以決定因應的優先順序；最後(三)執行風險控制，藉著建立風險因應團隊、實施權責分工、和考量內外的支援資源環境，進而擬定各項因應辦法、建立全套因應計畫。

步驟一、風險確認

一個機關的資訊通訊之運作可能遭遇人爲或自然因素之危害性因子而導致停機或不能正常作業的可能機率。風險是一種機率，且具主觀性。我們本就都處在一個非零風險的環境中。

可能造成作業平台停機或不能正常作業的行爲或事件，導致無謂的損失者。如電腦病毒、網路駭客、竄改資料、電腦故障、磁碟毀損、人爲故意或非故意的操作失當、……等，稱爲風險的危害性因子。可分兩類：(一) 其來自外在的稱爲威脅，如：未經授權的存取或使用資訊、資訊系統等資源，可能導致資訊的機密性、完整性或可用性受到破獲；火災可能威脅到資訊資產的可用性及完整性；偷竊可能威脅得資訊資產的可用性及機密性。(二)其來自資訊資產本身的稱爲弱點或缺失，如：實體環境缺乏適當保護、密碼未適當的選擇及保護、資安教育訓練不足等，足以可能被威脅事件所利用，而對資產產生傷害。

就資訊業務的風險而言，風險危機來源有人員、建築物、空調設備(包括空調、冰水機、出風口與迴風口)、電力設施(包括 UPS 不斷電設備、AVR 穩壓器、電力機房設施)、病毒(包括駭客攻擊、病毒)、網路通訊、硬體、軟體及廠商交貨等電腦暨相關輔助設施，遇到零件毀損、錯誤的系統設定或操作、應用系統程式錯誤、人爲經意或不經意的破壞、自然地震水災、火災或攻擊、廠商交貨期限延誤等危害因子發生，則可能產生服務中斷、當機、資料外洩等衝擊，繼而引發信譽或法律賠償的危機，如圖 5。

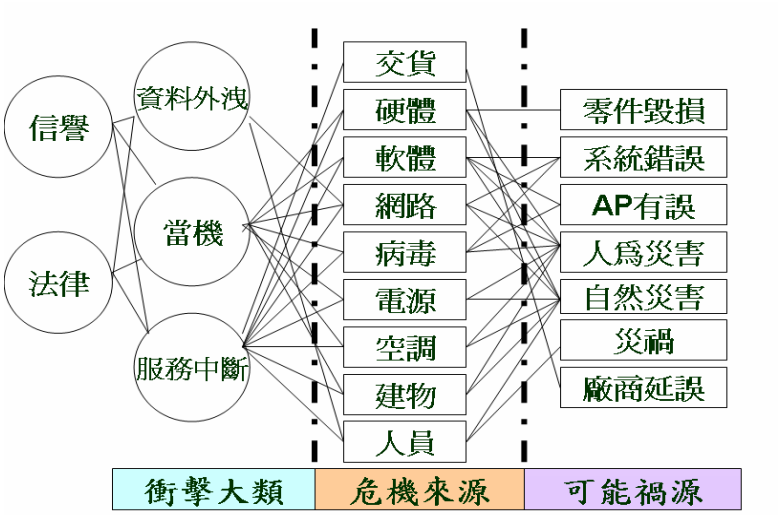

圖 5、資訊風險來源

剝析資訊業務的風險所在，始能依據衝擊程度排定風險管理的優先順序，並衡酌可容忍的程度和可投資的尺度，以規劃因應措施使降底風險發生的概率，並藉因應措施的完整性，發展一套資訊業務的緊急回復計畫。

資訊業務的風險確認步驟有二：

(一)成立風險管理團隊：至少副主官領軍，成員由資訊單位及各資訊系統的業務單位組成，分工負責所管業務，並由資訊單位總成。如圖 6。

圖 6、風險管理專案小組編組與工作要項

(二) 資訊資產全面清查：資訊單位擬定資產風險清查表，業務單位據以清查與業務應用系統相關資料如該系統與資料的重要程度、最大忍受服務中斷的時間、作業週期、作業尖峰期、備份方式、開發與維護方式等；而資訊單位除亦需配合瞭解該項業務所涉之軟硬體工具與平台之外，亦應就整體機房設施及人員作資產的盤點清查。如表 1。

表 1、資訊資產風險清查表

項目	內容
部門	
系統名稱	
業務負責同仁	姓名：　　電話/手機：
系統開發方式	□自行開發　□委外開發
系統維護方式	□自行維護　□委外維護
系統平台	名稱：＿＿＿＿＿＿ 內部負責同仁：＿＿＿＿＿＿ 維護廠商：＿＿＿＿＿＿ 聯絡人：＿＿＿＿＿＿ 電話/手機：＿＿＿＿＿＿
系統平台及版本	□ Windows，版本：＿＿＿＿＿＿ □ Linnix，版本：＿＿＿＿＿＿ □ Unix，版本：＿＿＿＿＿＿ □ 其他：＿＿＿＿＿＿　版本：＿＿＿＿
資料庫平台	名稱：＿＿＿＿＿＿ 內部負責同仁：＿＿＿＿＿＿ 維護廠商：＿＿＿＿＿＿ 聯絡人：＿＿＿＿＿＿ 電話/手機：＿＿＿＿＿＿
使用軟體	程式語言或工具
業務重要性程度	□1 □2 □3 □4 □5（由小而大）

衝擊嚴重性程度	□1 □2 □3 □4 □5（由小而大）
最大忍受中斷時間	□1hr □2 □3 □4 □8 □36 □48 □72hr
作業週期	□日 □週 □月 □半年 □年
作業尖峰期	□每年月份 □其他_____
備份方式	□即時備份 □定期備份
回復演練週期	□半年至少一次 □一年一次 □未曾演練

步驟二、風險評估

經過資訊整體業務的全面清查後，就可以進行風險評估，以排定風險控管的優先順序，和清楚瞭解風險管理的重點。風險評估的程序爲：

(一）重要資產之釐定

由於資訊資產繁多，勢需釐出重要資產(或稱關鍵性業務)，舉凡與機關的主要業務相關者，或業務停頓將引發民怨者，甚至於影響國計民生者等皆屬之。從重要性資產切入，繼而考量該項資產所在的平台的脆弱與否，使能擴及兼顧軟體與其硬體載具的風險檢查。

將所有業務資訊系統或資料清查，彙整得一覽表；再由各科室主管開會針對重要系統或資料討論確認先後次序；其次評估該等重要系統或資料所在之軟硬體平台之危害性因子。

如表 2，將重要性的等級分爲極重要、很重要、重要和普通等四級，分別賦予 7、5、3、1 的權重。

表 2、重要資產等級定義

等級	重要級	定義
極重要	7	當該項業務停頓 4 小時，將 1.影響民眾利益與民眾不安 2. 產生其他系統的骨牌效應達 85%以上 3. 引起主管機關及媒體的關注 4. 無法人工替代作業
很重要	5	當該項業務停頓 8 小時，將 1.引起民眾不安

		2.產生其他系統的骨牌效應達 65%以上 3.引起主管機關的關注 4.無法人工作業替代
重要	3	當該項業務停頓 72 小時，將 1.產生其他系統的骨牌效應達 30%以上 2.引起內部主管的關注 3.部分無法人工作業替代
普通	1	當該項業務停頓 72 小時，將 1.產生其他系統的骨牌效應達 30%以下 2.可以人工作業替代，或不致產生問題

（二）危害性因子之鑑定

首先條列可能的危害性因子，譬如火災、水災、人爲疏失（包括操作過失）、人爲竊取或破壞、病毒感染、駭客侵擾等，依關鍵性系統所在的平台之安全環境程度賦與各危害性因子 1 至 5 的危險等級，如表 3，A、B 系統在甲平台上，而甲平台的各種危害性因子的危險等級分別爲火災、水災和人爲疏失的發生率很低，故給值爲 1，人爲破壞、病毒感染、和駭客侵擾發生的可能率爲 3。

表 3、危害性因子可能發生頻率

資產	火災	水災	人爲疏失	人爲破壞	病毒感染	駭客侵擾
甲平台	1	1	1	3	3	3
乙平台	2	2	1	3	4	3

（三）危害衝擊影響之評估

1.依各平台之應用系統賦與重要等級，估算風險係數 (=重要等級 x 發生頻率)。

2.計算總分，如表 4，A 系統得 60、B 系統得 48。

表 4、衝擊影響之評估

關鍵性系統	危害性	火災	水災	人爲	人爲破壞	病毒感染	駭客侵擾	風險係數總	
	發生頻	1	1	1	3	3	3		甲平台
	要等級								
A 系統	5	5	5	5	15	15	15	60	
B 系統	4	4	4	4	12	12	12	48	
	重要等級	2	2	1	3	4	3		乙平台
C 系統	3	6	6	3	9	12	9	45	
D 系統	4	8	8	4	12	16	12	54	

（四）風險等級之評估

3.彙整比較各應用系統之風險係數總計，如表 5。

4.A 系統得 60，B 系統得 48 ， C 系統得 45， D 系統得 54

表 5、風險等級之評估

關鍵性系統	重要等級	所在平台	風險總計	優先順序	因應方案
A 系統	5	A	60	1	方案 1
B 系統	4	A	48	3	方案 3
C 系統	3	B	45	4	方案 4
D 系統	4	B	54	2	方案 2

（五）風險評估報告

最後，撰寫『風險評估報告』。

風險評估是一種物性的量化，量化的目的在以顯現風險高低爲原則，所以量化的數值可以視需要作合理之擬設。評估的項目以衝擊安全的項目爲考量，無論物性或非物性的項目都可以涵蓋在內，如有必要則需簡化，選擇重點即可。

風險評估的公式大都以線性函數思考，如正比關係或反比關係，倘能在既有公式之下更能顯現亦無不可；較正確的公式關係是來自試驗結果之推

估，並找出關鍵常數，困難度較高。

風險評估是安全的基點，從安全的風險評估可以窺見資訊通訊硬軟體建置及其環境與相關人員的缺漏與不足之處，和補強的思考，也可以藉此讓重要的業務或資訊獲得正確的保護，並能更以備援計畫作永續經營的憑藉。

步驟三、風險控制（擬定因應方案）

經過風險評估，產出『風險評估報告』，據以擬定各項業務的緊急應變回復計畫。

一個完整的緊急應變回復計畫（以下簡稱「緊急回復計畫」），應具備：(一)重要資料已經異地存放；(二)建立異地備援中心(成本高)，或與其他電腦中心相互支援(花費少)；(三)一份緊急通知名單已放置機房；(四)單位備妥計畫；(五)定期分項或全套測試，及隨時更新計畫內容。

緊急回復計畫文件內容至少應詳載下列資訊，作爲緊急應變時的依循：

（1）緊急狀況通報名單及程序 (包括啓動的宣佈者)
（2）緊急狀況小組之成員與責任 (包括發言人)
（3）回復小組之責任及處理程序
（4）異地存儲備份磁帶之目錄、地點及內容說明
（5）重要的應用程式及處理流程
（6）與支援中心的合約(同意書)，含處理程序、提供內容…
（7）主要的使用者的人工替代作業程序與表單樣本
（8）硬體、網路等物品清單
（9）回復計畫的維護程序記載，宜易於瞭解，利於執行

陸、結論

簡言之，風險管理是預防風險發生的方法工具，它是過程，產製一套風險控制的緊急應變回復計畫，並付之測試演練，才能達到風險管理的真正目標。

（本文轉載自主計月刊第 639 期<3 月>）

（本文由行政院主計處電子處理資料中心研訓組組長黃芳川 提供）