

曾經發生過…



- 有**350**家企業於**1993**年炸彈攻擊事件中在世貿大樓營運
- 其中有**150**家長達一年無法營運

再度發生...

Services | Contact | Site Map | Marketing

Contingency
Planning & Management
ONLINE

www.ContingencyPlanning.com

Site-Wide Search Find It!

Welcome! > Magazine > Article Archives October 2001

- By Richard Corcoran, Manager, Global Business Continuity, Eastman Kodak Company
 - http://www.contingencyplanning.com/article_index.cfm?article=393



ARTICLE ARCHIVES [Home](#)

Lessons Learnt from 911

by: Richard Corcoran
Pages: ; October, 2001

I participated in two Gartner conference calls that were set up to cover the numerous calls they were receiving from their clients regarding the September 11 disasters. Each call was attended by about 150 participants, as well as representatives from IBM, Comdisco, and SunGard (the three largest providers of contracted disaster recovery services). The conference calls took place on September 17 and 18.

摩根史坦利的危機應變

- 當**8:48分**第一架飛機撞上世貿大樓時，安全主管在一分鐘後緊急廣播，員工立即進行疏散
- **9:15分**在Seventh Avenue設立應變指揮中心，於九點二十五分啟動位於Varick街的資訊備援中心與建立位於紐澤西州Harberside的第二辦公室，恢復各系統運作。
- 該公司**9:03分**即**啟動企業備援計畫**疏散3500名員工，**9:50分**全部員工疏散完畢，9分鐘後大樓全部倒塌。
- 在**關鍵時刻立即啟動營運持續計畫**，成功的保護了公司最重要的資產及員工的生命。由於營運復原迅速，讓客戶的權益完全受到保護，除維持對客戶的承諾，更建立了長遠的信任關係。
- **危機應變成功重要因素：**
 - 發生時，員工被授權作決策，不須請示高層主管。使得3500名員工能在第一時間下樓。
 - 意外發生時，利用預先規劃的備援網路及電話線，成功的向員工及外界報導現況，維持通訊及指揮系統的暢通。
 - **事先規劃的設備清理計畫，該公司的電腦備援系統順利的在9:25分即開始運作，電腦中斷時間不超過1個小時**

發生在別人身上的…

- 2005年卡崔娜（Katrina）為美國史上登陸第三強之颶風
- 整體證實死亡統計人數為656人(至09/13止)。受災人數約二十七萬。整體損失將達3,000 億美元
- 紐奧良市堤防設計無法對規模三以上之颶風提供保護
- 紐奧良市80%地區遭水淹沒
- 約四萬五千位災民聚集在超級巨蛋及會議中心
- 經濟影響：油價、重建經費、保險理賠、物價的波動
- 災民的安置問題
- 救援物資的運補問題
- 後續重建問題



也曾發生在我們身上…

- 2001年9月納莉風災，台北捷運停駛三個月，交通黑暗期半年之久，北市政府共損失22億元
- 南港軟體園區停擺一個半月
- 四家固網業者及六家行動電話業者均無一倖免，電信機房與網路設備紛紛傳出災情
- 2009年8月8日，莫拉克風災造成南部、東部嚴重災情



天威難測...

- 1999年921大地震全台受創...
- 台積電雖然遭受重創、停電等影響，然事前已就各種災害事故研訂緊急應變、災害復原與營運持續等計畫，因此可以向客戶作「交貨不會延誤！」之保證。
- 其作法贏到的不只是訂單，而是更是長遠的信任感，促使企業永續經營。



神仙也幫不了...

- 2010年10月3日台塑集團南亞塑膠嘉義二廠三日上午，兩千坪廠房付之一炬，大火從白天燒到深夜...
- 南亞塑膠嘉義廠火勢從早燒到晚，延燒超過十二小時，不但臭味檢測超標四倍，持續濃煙也造成空氣中粒狀汙染物數值異常。下午突來的一場大雨，嘉義市、水上、中埔等鄉鎮紛傳降下像墨水般的黑雨....



簡報大綱

一、營運持續管理簡介

二、營運衝擊分析與風險評估

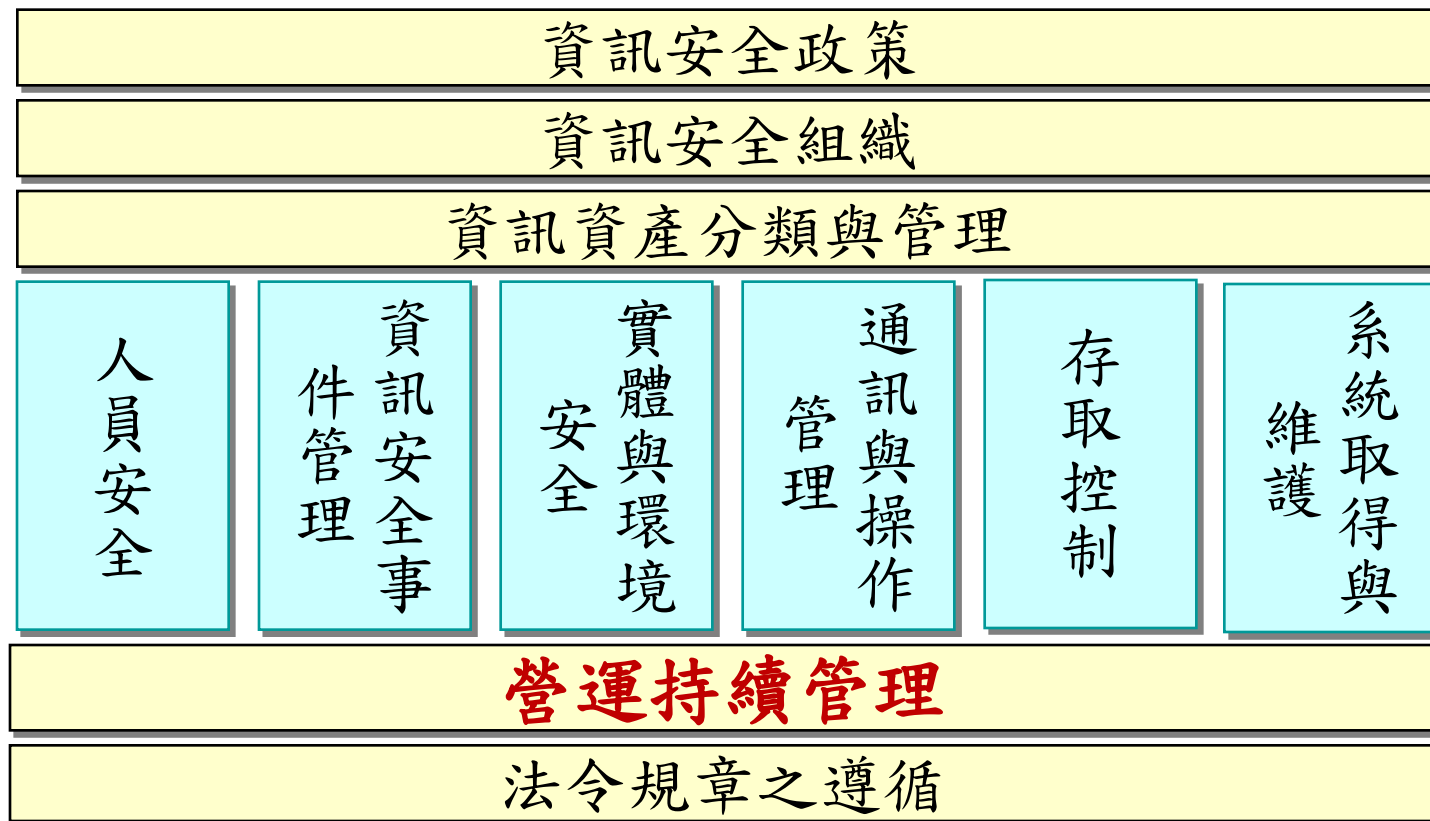
三、營運持續計畫擬定與實施

四、營運持續計畫測試與維護

五、範例與討論

ISO 27001對營運持續管理之要求

11 個領域、 39 個控制目標、 133 個控制要點



什麼是營運持續管理（BCM）

- 指的是企業在碰到任何天災人禍時，是否有**能力及策略**，繼續公司的營運。
- 現代企業**數位化的程度愈來愈深**，資訊系統差不多就是一般企業最薄弱的一個環節，病毒和停電算是小 case，火災算是中等的，但如果碰到地震？恐怖攻擊？
- 新加坡已經有國家標準，要求金融機構資訊系統不得斷線超過四個小時，日本也正在制定相關法律，不得斷線的時間同樣準備設定在四個小時...想想臺灣..

營運持續管理之目標

- 防止業務活動中斷，確保**重要業務流程**不受重大故障和災難的影響。
- 結合預防和復原措施，將風險造成的影響降低到**可以接受**的等級。
- 分析災難、安全缺失和服務損失的後果。制訂和實施**應變計畫**，確保在要求的時間內恢復業務流程。
- 選用**控制措施**降低風險，限制破壞性事件造成的後果，確保重要作業能及時復原。

營運持續管理相關計畫

營運持續計畫（BCP）

負責在遭到破壞或系統中斷後支持組織的業務功能。

災難復原計畫（DRP）

用於災難事件，在一段時間內對正常設備不能使用的情況下，在異地復原目標系統或IT設備的運轉。

營運持續計畫 vs. 災難復原計畫

營運持續計畫

策略性

技術性



業務運作

資訊運作

災難復原計畫

BCP(營運持續計畫) vs. DRP(災難復原計畫)

- Business Continuity Plan (BCP)
 - Business continuity planning is best described as the **process and procedures** that an organization can put in place to ensure that essential business functions continue to operate **during and after a disaster**. By having a BCP, organizations seek to prevent interruption of mission critical services. This type of planning enables them to re-establish services to a fully functional level as quickly and smoothly as possible. BCPs generally cover most or all of an organization's critical business processes and operations.
- Disaster Recovery Plan (DRP)
 - As **part of the business continuity process** an organization will normally develop **a series of DRPs**. These are more technical plans that are developed for specific groups within an organization to allow them to recover a particular business application. The most well known example of a DRP is the Information Technology (IT) DRP. Other traditional areas requiring specific DRPs include call centers, warehouses, distribution centers and any other areas of specialized activities.

BC vs. DR

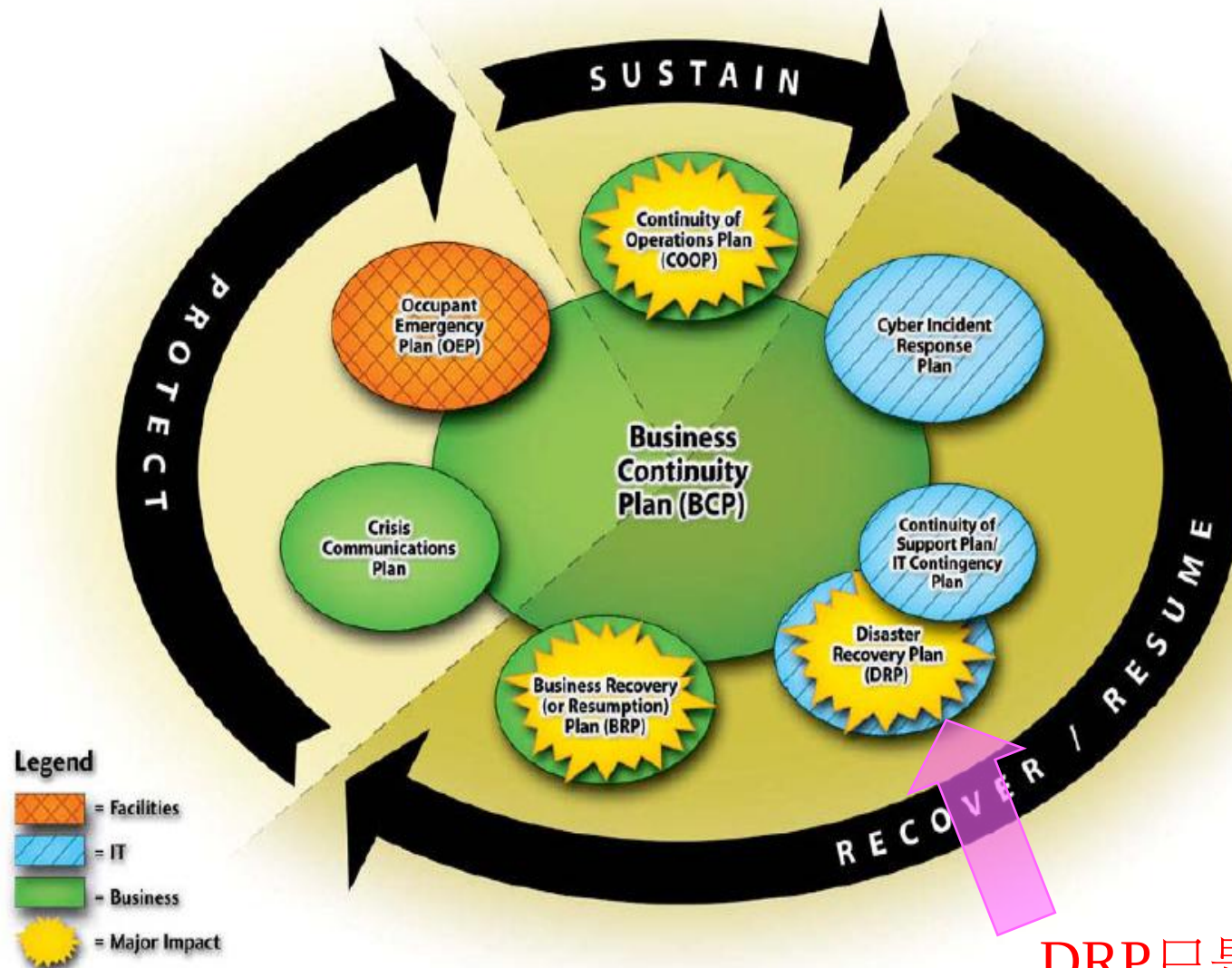
■ Business Continuous

- 研析並降低人為或是意外因素對重要業務運作可能導致的威脅，使重要業務在系統發生事故、設施失敗或是受損害時，仍可持續運作
- 目標是企業可以在經歷災難時或後，還能持續運作

■ Disaster Recovery

- BC的一環
- 著重在災難中復原 (Recovery)，進行resources redundant & backup, emergency response, and recovery
- 期望縮短災難發生對營業中斷的影響時間(加速復原)

BCP vs. DRP



DRP只是一小部份

一、營運持續管理簡介

二、營運衝擊分析與風險評估

三、營運持續計畫擬定與實施

四、營運持續計畫測試與維護

五、範例與討論

營運持續管理流程



營運衝擊分析

- 原文：Business Impact Analysis，簡稱BIA。
- 衡量意外災難如果發生，它對系統的破壞會造成組織多大的損失。
- 可以用定量化或定性化的方法進行分析。
- 徵詢管理至使用者階層對資源的使用需求，來判別其依賴程度和重要性。
- 應建立方法，用以決定支援主要產品與服務的業務活動中斷時之影響。

營運衝擊分析之目的

- 依照重要程度來定義不同作業程序的重要次序。
- 定義各系統的最大可容忍停機時間；又或稱之為目標修復時間。
- 在組織內形成營運持續的資安共識。
- 提供管理階層在訂定業務持續性策略和購置支援設備時的參考資料。

營運衝擊分析之步驟

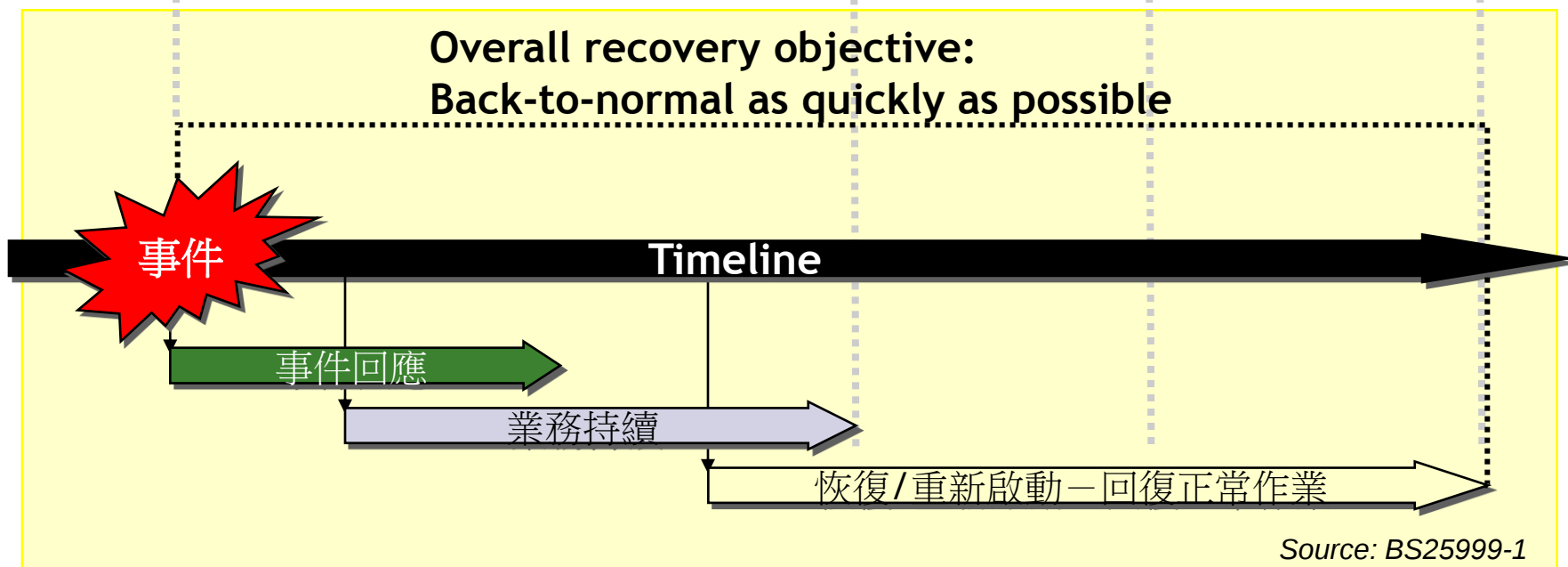
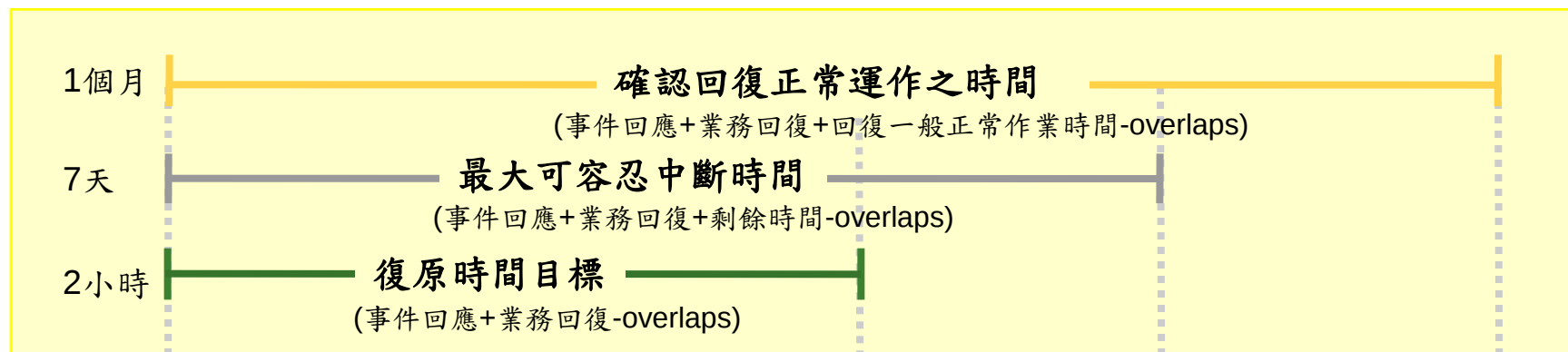
- 確認組織核心業務。
- 確認核心業務所需資源。
- 確認可容許中斷時間和衝擊影響。
- 確立修復優先次序。



RTO、RPO與MTPD

- RTO (Recovery Time Objective) 目標回復時間
 - ❑ 組織內主要之功能組織在經BIA辨識後所訂定之恢復最低的生產或服務水平目標所需之時間。
 - ❑ 備援系統取代原有系統開始提供服務所需的時間
 - ❑ 災難發生、系統中斷服務後，一直到系統恢復運作所需的時間(可容忍的系統中斷服務時間, recovery speed)
 - ❑ 從事件中恢復產品、服務或活動的交付的時間指標。
- RPO (Recovery Point Objective) 目標回復時點
 - ❑ 備援系統取代原有系統開始提供服務時，在資料上所能回復到的可用時點
 - ❑ 災難發生前，最近一次資料備份/複製成功的資料時點(可容忍的資料損失, data loss)
 - ❑ 系統回復服務時，資料所能回復到的可容忍時點
- MTPD (maximum tolerable period of disruption)最大可忍受中斷時間
 - ❑ 如果產品或服務的交付不能恢復，組織生存能力將受到不可恢復的傷害之最大時間。

事件發生與營運中斷時間之關係



營運持續管理策略之選擇

- 規避：改變或終止服務、產品以避開風險。
- 轉移：建立合約或協議(SLA)將風險轉移至另一個組織或機制。
- 接受：客觀的接受風險之存在，暫不加以控管。
- 降低：選擇適當之控管措施以減少可能之損失。

營運持續管理策略之考量重點

- 資源分配
- 可行性分析
- 替代方案
- 成本效益分析
- 建議方案
- 管理階層之認可



策略選擇範例

	異地備援	核心作業系統重建	人工作業
災害規模	區域性重大災害	局部輕微災害	全域特殊災害 (例如：電磁攻擊)
設備數量	僅容許使用重要設備	設備復原之數量較有彈性	設備需求較低
系統複雜度	僅容許選擇核心業務系統	復原時間及專業支援度	系統需求低
建置成本	高	中	低

策略選擇範例(續)

Site	Cost	Hardware Equipment	Telecom-munications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

NIST 800-34 Contingency Planning
Guide for Information Technology Systems

業務流程衝擊分析表範例

業務流程	單位名稱	負責人	流程/系統說明	衝擊影響	最大可容忍中斷時間(MTPD)	復原時間目標(RTO)	資料復原時間目標(RPO)	重要分級	備註
網路服務	XX組	XXX			4小時	2小时	N/A	高	
客戶系統	XX組	XXX			8小時	4小時	12小時	高	

一、營運持續管理簡介

二、營運衝擊分析與風險評估

三、營運持續計畫擬定與實施

四、營運持續計畫測試與維護

五、範例與討論

營運持續計畫內容

- 計畫啟動條件
- 職責說明
- 緊急程序
- 備援程序
- 復原程序
- 維護時間表
- 認知教育訓練



BCM 生命週期 (資料來源: BS 25000-1)

營運持續計畫宣導及訓練

- 計畫目標/作業標準
- 跨部門溝通協調
- 安全性考量
- 事件通報程序
- 個人責任與職責



預防性措施考量要點

- 實體性預防措施
- 資料備份
 - 資料備份系統
 - 替代性備援系統
 - 系統備品
- 人員管理
 - 人員角色和責任
- 預防成本 VS. 應變成本



營運持續計畫實施要點

- 確定各項應變處理程序及權責。
- 與廠商或客戶間業務關係及合約的適切性。
- 處理程序及流程應文件化。
- 進行適當的員工訓練。
- 檢查並更新計畫。
- 計畫應著重具體的業務目標方面。
- 確定所需服務和資源，包括人員、非資訊處理資源的相關資源，以及資訊處理設備等項目。

應注意事項

- 相關單位之配合。
- 公告執行日期與時間。



一、營運持續管理簡介

二、營運衝擊分析與風險評估

三、營運持續計畫擬定與實施

四、營運持續計畫測試與維護

五、範例與討論

測試方法

- 檢查表測試：
 - 提供檢查表予相關人員檢視程序內容，並視實際狀況提出修正建議。
- 書面測試：
 - 集合相關人員共同檢視業務永續運作計畫。
- 模擬測試：
 - 以模擬環境進行業務永續運作計畫測試。

測試方法(續)

- 平行測試：
 - 在備援平台上進行測試。
- 完全測試：
 - 於實際作業環境中進行業務永續運作計畫測試。

測試範圍及影響評估

- 有效性及風險
- 流程數量
- 系統數量

定期檢視

- 定期檢討可用性
 - 實體環境
 - 安全性/技術性
 - 軟硬體設備/替代方案和備援系統
 - 人員
- 檢視外部支援的資源狀況
 - 委外廠商合約
 - 軟體合法授權
 - 異地備援中心
 - ...

定期檢視(續)

- 定期檢討遵循性
 - 相關法規
 - 營運策略
 - ...
- 定期檢視營運風險變化
 - 作業面
 - 財務面
 - 技術面
 - ...

不定期檢視

- 組織營運策略變動時。
- 採購新的設備，或是更新作業系統。
- 使用新的問題偵測及控制技術（例如火災偵測）。
- 使用新的環境控制技術。
- 人員及組織上的調整變動。
- 單位、人員地址及電話號碼的異動。

不定期檢視(續)

- 契約當事者或是供應商的調整變動。
- 業務流程的變動，新建或是撤銷作業流程。
- 實務作業的變更。
- 法規上的變更。

再評估

- 各部門之災難復原計畫是否與營運持續管理之目標相符。
- 所有重要及關鍵性風險是否已辨識。
- 是否有完整確實之教育訓練。
- 是否有足夠之操作手冊。
- 是否確實掌握緊急應變之所有資源。
- 是否掌握組織最新資訊（人員及設備）。
- 是否掌握外界最新資訊。

營運持續計畫更新

- 再評估結果中前述各項因素改變，則應進行計畫更新。
- 更新計畫應依循原有程序進行各項作業。

一、營運持續管理簡介

二、營運衝擊分析與風險評估

三、營運持續計畫擬定與實施

四、營運持續計畫測試與維護

五、範例與討論

業務永續運作管理常見問題

- 異地備援場所空間不足
- 回復策略評估不正確
- 缺乏業務單位的參與，或未得到業務單位的同意
- 忽略部門或應用系統相依的關係
- 忽略部分重要資源（Internet、e-mail等），造成業務運作的瓶頸
- 支援的資源不足
- 回復計畫不夠詳細，仍需依賴熟析系統的人員執行
- 處理流程不明確，無法照表操課
- 缺乏適當的維護更新機制
- 通常只測試回復系統，缺乏完整流程測試

業務永續運作計畫演練活動紀錄(1/2)

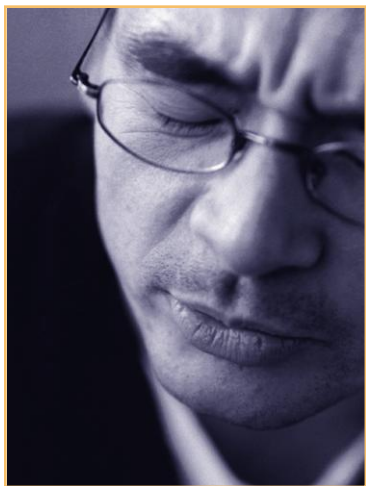
演練規劃表					
承辦人：					
協辦單位：					
規劃日期：					
演練規劃項目		規劃內容			
1	規劃演練目標與範圍				
2	規劃演練腳本				
3	規劃演練所需設備				
4	規劃演練所需系統				
5	規劃演練所需參與人員				
6	規劃演練時程及完成時限				
7	規劃演練測試方式與測試資源	☐ 書面流程演練 ☐ 通報演練 ☐ 關鍵業務流程之復原演練 ☐ 待資源充足後安排進行演練測試			
8	規劃演練成果檢討				
承辦人		單位 主管		日期	

業務永續運作計畫演練活動紀錄(2/2)

演練暨處理執行表					
承辦人：					
協辦單位：					
演練日期：					
計畫開始時間				計畫需要時間	
計畫結束時間				實際作業時間	
演練執行項目		執行程序		負責人	執行結果
1					開始時間： 時 分 結束時間： 時 分 ☐ OK ☐ NO
2					開始時間： 時 分 結束時間： 時 分 ☐ OK ☐ NO
3					開始時間： 時 分 結束時間： 時 分 ☐ OK ☐ NO
4					開始時間： 時 分 結束時間： 時 分 ☐ OK ☐ NO
5					開始時間： 時 分 結束時間： 時 分 ☐ OK ☐ NO
結果檢討：					
承辦人		單位 主管		日期	

結論

- 業務永續運作管理可幫助組織通過關鍵考驗
- 業務永續運作管理不僅限於資訊層面，組織所有運作均應納入考量。
- 應定期執行業務永續運作計畫演練測試並依現況調整。
- 應落實宣導及教育訓練。



&

