IT災害復原簡介
(IT Disaster Recovery)

國家資通安全會報 技術服務中心

江衍勳

Mar. , 2009

大綱

- 前言
- 新聞事件
- 營運持續管理簡介
- IT災害復原簡介
- 結論

前言

- 自2001年美國9/11恐怖主義攻擊事件、2003年全球SARS病毒侵襲事件，乃至於全世界瀕臨大規模爆發邊緣的禽流感事件，在在凸顯出風險管理及危機處理的重要性
- 根據美國「國家檔案保存及紀錄管理局」(National Archives and Records Administration)統計結果顯示：93%的企業組織，若其資料中心發生災難超過九天，仍無法恢復正常運作，一年內將破產倒閉
- 另外根據全球性研究機構「策略研究協會」(Strategy Research Institute)之研究顯示，企業組織若無法在發生災難十天內恢復營運，其之後的存活可能性極低

前言(續)

- 在現今高度競爭與服務導向的社會當中，任一公民營單位的關鍵性業務及日常營運流程皆高度依賴IT系統。如何在IT系統發生運作中斷時，能於事先訂定及必要的回復時間內，採取系統性的程序與步驟，恢復相關系統之正常運作，進而使業務流程恢復運行，此即為「IT災害復原」(IT Disaster Recovery，簡稱 ITDR)之範疇
- 「IT災害復原」將是組織維持營運能力、提昇競爭優勢的重要管理方式與工具，用以達成組織營運持續之終極目標

新聞事件

- 新聞來源：中央社2009.1.10
- ○○○電腦當機36小時，不僅讓旅客在機場苦待，也造成8名列管人員入出境，探究原因，○○○雖然都指向電腦，但缺乏警覺、人員訓練不足和未做「第三地備援」才是肇禍主因
- 「第三地備援」為一般大型企業電腦必備的設備，用以確保資料安全無虞，所謂第三地，就是在第一主機和第二主機之外，還有一個備份主機放在安全的第三地；○○○入出境電腦資料相較大型企業更形重要，因為牽涉到恐怖分子列管、國內外通緝列管的重要國家安全問題

4

新聞事件(續)

- 2001年納莉颱風時，○○銀行位於的台北作業大樓的電腦主機因發電機淹水而無法運作，資訊處立刻於當天啟動位在台中的異地備援主機，供各分行連線使用。於短暫的時間內恢復正常運作。所依賴的正是平日慎密的規劃及不斷的測試演練與檢討

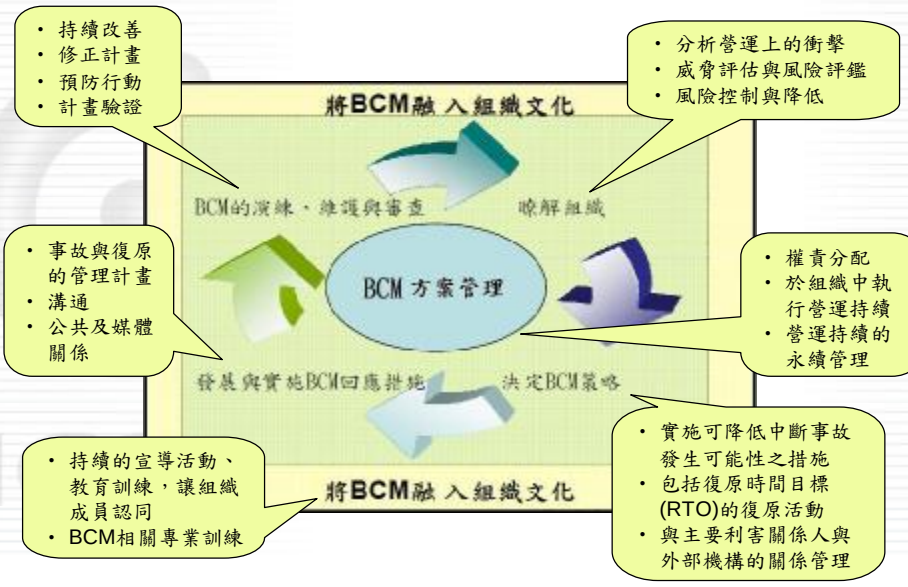
5

營運持續管理簡介
(Business Continuity Management;BCM)

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

營運持續管理架構



8

營運持續管理架構(續)

Ÿ BCM包含多種類型計畫，其各類型計畫可依照計畫目的、應用範圍與適用狀況不同而可用分階方式來建立

上層計畫可為下層計畫之通用指導管理原則

9

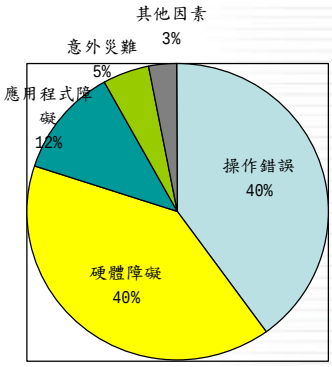
IT災害復原簡介
(Information Technology Disaster Recovery)

IT災害復原定義

- IT災害復原意指回復組織被中斷的IT與通信能力，確保重要業務運作得以持續
- IT災害復原計畫(ITDR Plan)是一份載明當災害發生時，回復IT與通信能力之文件。內容包括主要參與人員、資源、服務及需要執行的行動方案

災害發生後造成系統中斷時間分析

- 造成系統中斷，各因子所佔中斷時間(Downtime)之比率分析
  - 40% 操作錯誤(operation error)
  - 40% 硬體錯誤(hardware error)
  - 12% application failure
  - 5% disaster
  - 3% other environmental

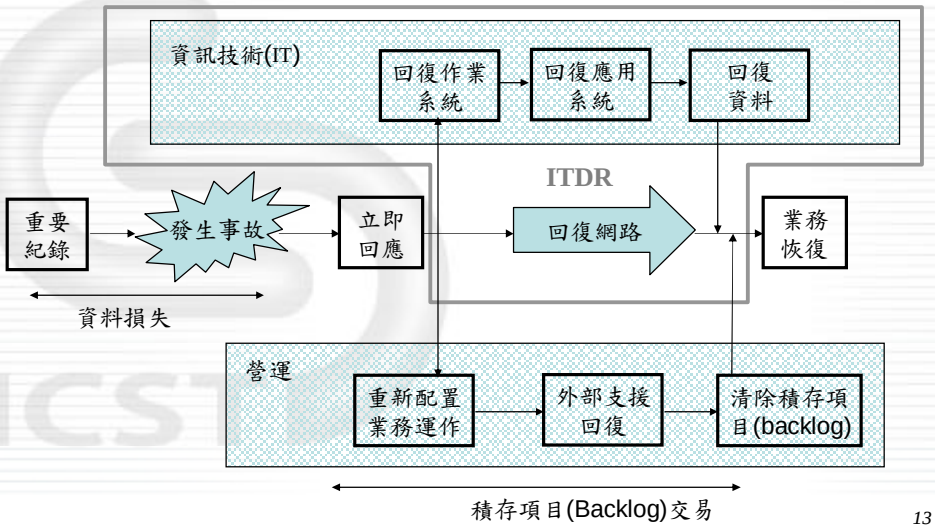


- 80%的Downtime是因為人為操作錯誤或是硬體障礙，這也是為何要強調Procedure & Plan

12

BCM與ITDR的關係

營運持續管理



13

規劃IT災害復原6大領域

風險分析與檢視(Risk Analysis & Review)

⇩

系統衝擊分析(System Impact Analysis)

⇩

IT災害復原持續策略(ITDR Continuity Strategy)

⇩

IT災害復原計畫發展(Development of ITDR Plan)

⇩

IT災害復原測試與演練(ITDR Test & Exercise)

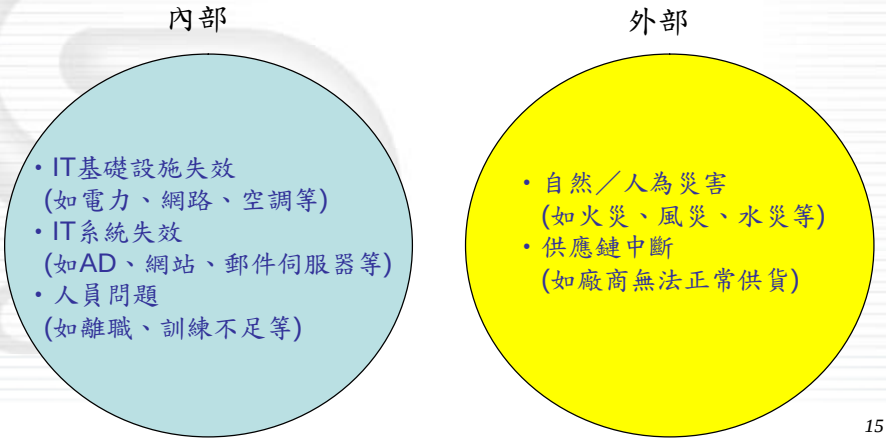
⇩

方案管理(Programme Management)

14

風險分析與檢視

Ÿ 經由對內部與外部作業環境的風險分析與檢視，發覺組織在IT方面潛藏的風險



15

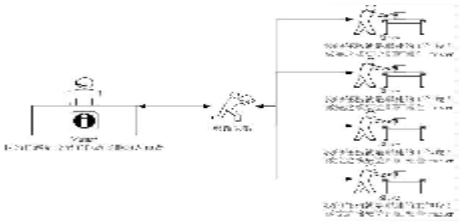
風險分析－降低風險措施

- 硬體失效&降低風險措施
  - 電力失效
    - 電擊防護
    - 預防維護與定期測試
    - 自動切換開關與發電機
  - 混亂環境
    - 正確的標示與接線
    - 定期維護
  - 高溫
    - 環境監控
    - IT專用的空調系統

16

風險分析－降低風險措施(續)

- 硬體缺陷(Faulty Hardware)
  - 熱待機設備(Hot Standby Device)
  - 高可用度的叢集架構
  - 適時的系統檢視
- 軟體失效&降低風險措施
  - 測試環境
    - 上線前驗證
    - 在虛擬環境(如VMWare)下測試
  - 資料整合-回復失效
    - 資料備份與程序
  - 安全組態
    - 防火牆規則與存取
    - 適當的資料庫存取



17

風險分析－降低風險措施(續)

- 網路組態
  - Ø 適當的通訊組態
  - Ø 疑難排除工具
- 應用系統與作業系統版本
  - Ø 定期修補程式更新
  - Ø 重大修補程式立即更新
  - Ø 部署修補程式前之測試

Ÿ 病毒感染&降低風險措施

- 掃毒軟體
- 定期掃描

18

風險分析－降低風險措施(續)

Ÿ 駭客入侵&降低風險措施

- 合作廠商的安全檢視
- 適當的防火牆組態
- 入侵偵測/預防軟體
- 保持軟體修補程式在最新狀態
  - Ø 作業系統
  - Ø 資料庫
  - Ø 應用程式
  - Ø 韌體(Firmware)

Ÿ 實體破壞&降低風險措施

- 門鎖
- 生物辨識
- 攝影監視與移動偵測感應

19

風險分析－降低風險措施(續)

- 人為錯誤&降低風險措施
  - 單點失效
    - 交叉訓練
    - 文件化
    - 代理人制度落實
  - 訓練不足
    - 定期訓練與檢定

風險分析應注意事項

- 風險分析應包括所有使用中的IT設施
- 依據各項風險分析結果，實施保護措施
  - 避免或降低事故發生的可能性
  - 降低傷害所造成的損失
- 風險分析應至少每年實施1次

規劃IT災害復原6大領域

風險分析與檢視(Risk Analysis & Review)

⇩

系統衝擊分析(System Impact Analysis)

⇩

IT災害復原持續策略(ITDR Continuity Strategy)

⇩

IT災害復原計畫發展(Development of ITDR Plan)

⇩

IT災害復原測試與演練(ITDR Test & Exercise)

⇩

方案管理(Programme Management)

22

系統衝擊分析

- 當關鍵資訊系統面臨之資安威脅已影響到關鍵業務與服務之運作時，檢視與分析其潛在衝擊之程序
  - 系統衝擊分析應辨識以下項目
    - 關鍵IT伺服器
    - 關鍵IT應用系統
    - 關鍵網路通訊需求
    - 關鍵資料
    - 重要紀錄
    - 各項關鍵IT系統之回復時間
    - 最低資源需求

23

影響系統衝擊分析的因素

- 財務的影響，包括可能帶來的異常費用損失
- 作業的影響
- 重要的營運程序、應用及資料
- 回復的技術需求
- 營運單位(Business Unit)對IT資源的相互依賴程度

24

系統衝擊分析的作法

- 辨識各項處理系統的重要性(Criticality)，亦即系統運行中斷時，造成的損失→**How Much**
- 中斷發生後多久時間內會帶來影響→**When**
- **Criticality = How Much + When**
- 重要性將決定以下項目：
  - 規劃可接受程度(Acceptable)的回復需求
  - 決定花費多少預算在回復能力上
- 分析結果可以量化與非量化表示(範例)
  - 量化：如收入損失、罰款等
  - 非量化：如形象損失、喪失商機等

25

系統衝擊分析應注意事項

- 針對IT進行之系統衝擊分析結果，將依據其優先順序實施復原作業
- 系統衝擊分析不只是考量系統自身的價值，亦應考慮對其他業務所造成之影響
- 系統衝擊分析階段易遇到抗力與阻礙，惟有高階管理者的支持，始得以降低或克服這些阻抗

26

規劃IT災害復原6大領域

風險分析與檢視(Risk Analysis & Review)

⇩

系統衝擊分析(System Impact Analysis)

⇩

IT災害復原持續策略(ITDR Continuity Strategy)

⇩

IT災害復原計畫發展(Development of ITDR Plan)

⇩

IT災害復原測試與演練(ITDR Test & Exercise)

⇩

方案管理(Programme Management)

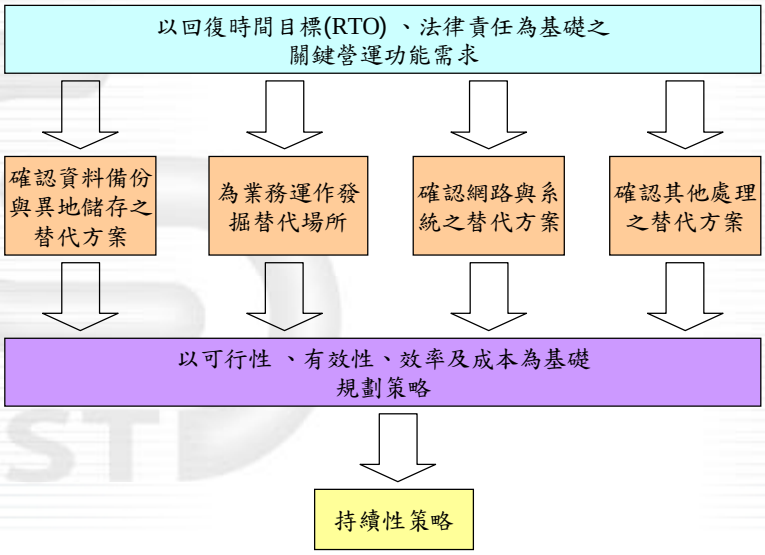
27

IT災害復原持續策略

- 依據系統衝擊分析階段辨識之潛在損失衝擊，IT部門應謹慎選擇適當的IT災害復原策略，以保護其利益之程序
- 策略可以從以下項目探討
  - 方法論(Methodology)
  - 技術面(Technology)

28

IT災害復原持續策略－方法論



29

IT災害復原持續策略－技術面

- 系統備援
  - 熱備援場所(Hot Site)：擁有所需完整、設定好的硬體、軟體和各項必要的工作環境(如網路)，並隨時待命
  - 暖備援場所(Warm Site)：具備電源、空調、通信和高架地板等基礎設施，以及某部份的執行環境(某些硬體、週邊裝置)，但沒有完整的設備或軟體安裝
  - 冷備援場所(Cold Site)：只提供緊急事故時可以繼續運作的建築空間，擁有電源、空調等基礎建設，但沒有任何電腦硬體

30

IT災害復原持續策略－技術面

- 資料備份
  - 策略考量
    - Ø 備份排程完成後，要進行備份保存與存放位置規劃
    - Ø 要有完整之紀錄保存工作表，包含使用單位、種類、媒體形式、容量等相關資訊
    - Ø 備份媒體存放於何處對於備份回復所需之時間與努力有很大影響
    - Ø 但災難(例如火災）發生時，資料備份在上線環境可能也會損害，所以許多組織將備份資料異地存放

31

IT災害復原持續策略－技術面

- 資料備份
  - 備份方式：線上備份(On-Line Backup)
    - 在系統提供服務時，同時進行資料備分作業，亦即用戶仍可存取資料
    - 不必在營業時間外進行備份
    - 伺服器效能會受影響
    - 開啟的檔案可能無法備份
  - 備份方式：離線備份(Off-Line Backup)
    - 系統必須中斷服務或用戶暫停存取資料下進行備份
    - 具有較佳的備份效能
    - 可完整的備份所有檔案

32

IT災害復原持續策略－技術面

- 常見備份類型
  - 完整備份(Full Complete Backup)：備份所有資料至特定媒體(把全部檔案進行備份，並把已備份的檔案標示為已備份)
  - 增量備份(Incremental Backup)：只備份上次(增量)備份後有所變更或新增的資料(只備份經修改的檔案，或新建立但沒有標示為已備份的檔案，並把備份後的檔案標示為已備份)
  - 差異備份(Differential Backup)：只備份上次完整備份完成後有所變更的資料(只備份經修改的檔案，或新建立但沒有標示為已備份的檔案，但不會把已備份的檔案標示為已備份)

影片展示

33

IT災害復原持續策略－技術面

- 備份媒體
  - Ø 備份的資料量
  - Ø 備份時間間隔
  - Ø 作業環境
  - Ø 備份系統與儲存裝置的距離
  - Ø 成本與效能分析
  - Ø 儲存媒體：磁片(Diskette)、磁帶(Tape)、硬碟(Hard Drive)、光碟(CD-R / CR-RW / DVD)及其它(如行動碟)

34

IT災害復原持續策略應注意事項

- Ÿ 可行性
- Ÿ 要常見而不特殊
- Ÿ 要有效以滿足復原時間目標(Recovery Time Object)的要求
- Ÿ 成本
- Ÿ 安全、完整及可擴展性

35

規劃IT災害復原6大領域

風險分析與檢視(Risk Analysis & Review)

⇩

系統衝擊分析(System Impact Analysis)

⇩

IT災害復原持續策略(ITDR Continuity Strategy)

⇩

IT災害復原計畫發展(Development of ITDR Plan)

⇩

IT災害復原測試與演練(ITDR Test & Exercise)

⇩

方案管理(Programme Management)

36

IT災害復原計畫發展

- 依據選定之IT 災害復原策略，發展細部IT 災害復原計畫
- 計畫應明訂面臨潛在威脅的回應與回復，所需具備的資源與能力，例如：
  - 時程
  - 災害啟動、判斷及動員之程序文件
  - 重要紀錄恢復文件
  - IT系統回復程序文件
  - 網路與通訊文件
  - 應用系統與資料同步檢查表文件
  - 手動操作程序文件

37

IT災害復原計畫發展

- IT災害復原計畫細部構成要素，如
  - 災害復原場所的資源
    - 包括確保設備與人員可用之程序與檢查表
  - 備份程序
    - 備份方法
    - 同步程序
  - 回復程序
    - 逐步的(step by step)作法
  - 應用系統與終端使用者的測試
    - 系統回復是否正確
    - 資料同步的結果是否無誤
    - 測試的時程

38

IT災害復原計畫發展應注意事項

- 應文件化，並設定文件控管機制以避免版本誤用
- 應視業務、組織及人員的調整需求而進行維護更新，以確保計畫之有效性
- 應指定維護權責單位，且每年至少一次來評估，並將檢討與更新的結果送交管理階層審視與核定
- 需將更新後之結果通知全體相關人員

39

規劃IT災害復原6大領域

風險分析與檢視(Risk Analysis & Review)

⇩

系統衝擊分析(System Impact Analysis)

⇩

IT災害復原持續策略(ITDR Continuity Strategy)

⇩

IT災害復原計畫發展(Development of ITDR Plan)

⇩

IT災害復原測試與演練(ITDR Test & Exercise)

⇩

方案管理(Programme Management)

40

IT災害復原演練與測試

- 經由測試與演練，驗證已建立之IT災害復原程序，發展細部的IT災害復原計畫
  - 測試與演練計畫中可能曝露的錯誤與疏失
  - 提供計畫使用之資源，應測試其可存取性(accessibility)、可用性(availability)及適當性(adequacy)，確保回復程序的效率與有效性
  - 藉由演練，使相關同仁熟稔回復程序
  - 做為實際災害與回復情形之間的評量基準

41

IT災害復原演練與測試

- 執行災害復原計畫之演練/測試應有計畫與結果報告
- 演練/測試計畫應包含以下項目(計畫表)
  - 演練/測試腳本(假設狀況)
  - 演練/測試目標
  - 演練/測試範圍
  - 演練/測試時程
  - 參加人員
  - 預計演練/測試項目
  - 演練/測試方法
  - 演練/測試所需資源

42

IT災害復原演練與測試

- 演練/測試結果報告
  - 演練/測試完成後，應提出結果報告，報告內容應包含下列項目：
    - 執行時間與地點
    - 演練/測試過程紀錄
    - 參加人員
    - 演練/測試結果檢討

43

規劃IT災害復原6大領域

風險分析與檢視(Risk Analysis & Review)

⇩

系統衝擊分析(System Impact Analysis)

⇩

IT災害復原持續策略(ITDR Continuity Strategy)

⇩

IT災害復原計畫發展(Development of ITDR Plan)

⇩

IT災害復原測試與演練(ITDR Test & Exercise)

⇩

方案管理(Programme Management)

44

方案管理

- 維護IT災害復原計畫流通之程序
- 組織應該
  - 定期與系統化的檢視風險及業務／系統衝擊
  - 重新調整IT災害復原策略
  - 重新確認IT災害復原計畫的有效性
- IT災害復原計畫應成為組織運作與組織文化的一部分

45

方案管理

- 設定維護的政策
  - 內部稽核以定期實施各業務單位與資訊部門之回復計畫
  - 各項回復計畫的所有人及其權責
  - 對所有相關人員的認知訓練
  - 更新與檢視回復計畫之頻率
  - 定期測試回復計畫之頻率
  - 定期檢視供應商的回復計畫
  - IT災害復原計畫的版本控制
  - 與災害復原／營運持續服務提供者之合約協議

46

結論

- 在IT系統發生運作中斷時，如何在最快的回復時間內，使業務流程恢復正常運行，是各組織必須事先規劃完成
- 完成相關規劃後，最重要工作即是定期演練，藉此增加資訊系統負責人員對系統的熟識度與處理災害的應變能力，亦可驗證備份系統功能的完整性，可避免當災害發生時進行還原才發現備份資料未具完整性

47

附錄

系統衝擊分析範例

回復等級	系統名稱	系統描述	財務影響	可容忍最大中斷時間
1(高)	訂單/Web	以Web介面處理客戶訂單資料	$500,000/每日	1小時
2(中)	財務報表	產出各項財務報表	<$100,000/每日	3至5天
3(低)	差勤系統	登錄各項出勤紀錄	None	無關鍵時效限制

IT災害復原演練與測試－計畫表範例

IT災害復原(ITDR) 演練/ 測試計畫表	
執行單位：	協助單位：
計畫提出日期：	
演練/測試規劃項目	規劃內容
1 演練/測試之目標與範圍	
2 演練/測試腳本說明	請參考<IT災害復原演練/測試腳本規劃表>
3 演練/測試項目與執行方式	
4 演練/測試所需資源(例如軟體、硬體、場所、設施等)	
5 演練/測試所需參與部門與人員	
6 演練/測試執行日期	
7 演練/測試所需時間	
8 演練/測試結果之檢討時程	
計畫管理小組簽核：	
IT災害復原管理委員會簽核：	

50

IT災害復原演練與測試－腳本規畫範例

IT災害復原計畫(ITDRP)演練/測試腳本規畫表				
演練/測試假設狀況說明：				
時間	執行步驟	執行人員	執行所需資源	執行地點

51

IT災害復原測試與演練－報告範例

IT災害復原計畫演練/ 測試結果報告單	
演練/測試項目	
演練/測試部門	
演練/測試方式	
演練/測試實施日期	
演練/測試預計所需時間	
演練/測試實際作業時間	
演練/測試參加人員	
演練/測試結果檢討日期	
演練/測試作業步驟(請附上相關作業步驟執行紀錄或證據)	
演練/測試結果檢討：	
計畫管理小組簽核：	
災害復原管理委員會簽核	

52