教育部國民及學前教育署
112年度校園資通安全專責人員知能研習

資訊系統備份與回復演練

長榮大學
圖書資訊處系統管理
俞怡中

案例

學習歷程檔案硬碟被還原

https://www.youtube.com/watch?v=M-uMhLtQdX8&t=5s

公視新聞片庫遭刪除

https://www.youtube.com/watch?v=04DgxRp05nI&t=2s

備份很重要
備份很重要
備份很重要

備份是資安管理的**最後一道防線**

向上集中後 備份與演練的重點?

- 五大核心系統向上集中後
  - 備份的責任在集中端
  - 學校的權利與義務
    - 知的權利

      系統中斷後的回復時間

      備份週期

      資料回復測試
    - 監督的義務
      - **委外合約監督**

- 校內還有資訊系統嗎?
  - 主計系統
  - 財管系統
  - 舊的校務資訊系統
  - 個人電腦裡的資料
  - 網路設備
  - 資安設備
  - ……

  還是要做備份與資料回復測試

業務營運持續

業務營運持續管理

- Business Continuity Management，BCM
- **遭逢天災或人禍等意外時**，保護重要營運過程不受重大資訊系統失效或災害的影響，仍然可以繼續運作。
- 以**風險管理為基礎**，建立切合組織業務與目標的營運持續計畫，
- 依照適當的管理程序，**定期測試與維護**，使得營運持續管理不是紙上談兵而已，而是一套具體可行的方案。

營運持續演練 BCP

業務營運持續管理

- 營運持續管理透過預防與復原控制措施的組合，將組織的**衝擊最小化**，把**風險造成的影響降低**到可以接受的等級。
- 而在規劃過程中，必須了解組織面臨風險發生的可能性與衝擊，能夠鑑別出影響組織成敗的重要業務，
- 維運這些重要業務時所需要的資產，包括：人員、軟硬體、行政資源、通訊資源等。
- 根據**風險評鑑**的結果發展營運持續策略，以決定營運持續的整體作法。

營運衝擊分析

- BusinessImpactAnalysis，BIA
- 找出**關鍵業務、核心活動**。
- 鑑別出在中斷事件發生時，那些業務、活動會影響到組織的運作
- 進而降低中斷發生之可能性，準備。
- 並建立**緊急復原的機制**。

BIA vs 資通訊系統分級

- 資通安全責任等級分級辦法
  - 附表九資通系統防護需求分級原則
  - 鑑別系統等級：普、中、**高**
  - 識別**核心系統**
- 界定RPO、RTO
  - 上級要求：主管機關、學校長官
  - 使用者需求
  - 系統重要性
  - 資料變更的頻率

核心系統不限於【高】等級系統

業務流程/資訊系統	負責單位	負責人	復原時間目標（RTO）	資料復原時間目標（RPO）	系統等級	重要分級	備註
學術網路服務 / 學術網路連線	圖書資訊處(系統網路組)	[redacted]	4工作小時	N/A	中	高	
學術網路服務 / 網域解析(DNS)	圖書資訊處(系統網路組)	[redacted]	4工作小時	24小時	中	高	每日snapshot
校務行政作業 / 校務e化系統資料庫	圖書資訊處(軟體發展組)	[redacted]	4工作小時	6小時	中	高	每六小時備份一次
校務行政作業 / 校務e化系統應用程式	圖書資訊處(軟體發展組)	[redacted]	4工作小時	24小時	中	高	每天下班後備份一次
校務行政作業 / 學生系統應用程式	圖書資訊處(軟體發展組)	[redacted]	4工作小時	24小時	中	高	每天下班後備份一次
校務行政作業 / 選課系統應用程式	圖書資訊處(軟體發展組)	[redacted]	4工作小時	24小時	中	高	每天下班後備份一次
校務行政作業 / 學校首頁	圖書資訊處(系統網路組)	[redacted]	8工作小時	24小時	普	中	每日snapshot

RPO

- Recovery Point Objective，**可容許的最大資料損失量**
- 與**備份週期**有關
- 數值要如何界定：
  - 與組織能夠承擔的**風險**
  - 擁有的**資源**
  - **資料異動**的頻繁程度

EX

- 假設每天早上固定6:00備份，RTO為24小時

RTO

- Recovery Time Objective，**讓系統重新上線的時間**
- 系統回復所需的時間
  - 重新安裝? **映像還原**?
  - **設定檔案**
  - **資料回復**，最耗時的部分(有些認定RTO不含資料回復時間)

EX

- 上午8:00系統毀損後，在硬體設備沒問題的狀態下，下午2:00完成系統重建、資料回復，讓系統重新上限。RTO為6小時

MTPD

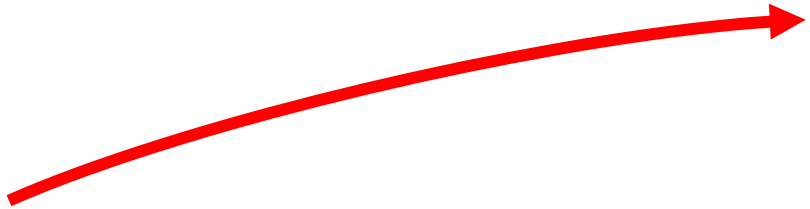
- Maximum Tolerable Periodof Disruption，**最大可容忍中斷時間**

- RTO把資料回復時間算入➔MTPD=RTO
- RTO不資料回復時間算入➔MTPD>RTO=RTO+資料回到時間

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間	資通系統分級
校務學生資料管理	校務行政系統(已向上集中文心機房)	為本校依組織法執掌，足認為重要者	1.違反法遵義務：依個人資料保護法，應善盡個人資料保護責任。2.影響校務運作	24小時	中
官網	官網(已向上集中至成功大學)	為本校依組織法執掌，足認為重要者	影響校務運作	24小時	中
網域管理系統	DNS (已向上集中至成功大學)	為本校依組織法執掌，足認為重要者	影響校務運作	24小時	中
電子郵件系統	已向上集中至教育雲	為本校依組織法執掌，足認為重要者	影響校務運作	24小時	中
學生學習歷程系統	學生學習歷程系統(已向上集中文心機房)	為本校依組織法執掌，足認為重要者	1.違反法遵義務：依個人資料保護法，應善盡個人資料保護責任。2.影響校務運作	24小時	中

業務持續演練 BCP

- 計畫
- 腳本
- 演練
  - 紀錄
    - 截圖
    - 紀錄時間
    - 資料回復
- 回復後測試與驗證
- 檢討



- 誰執行：
  - 自己做
  - 向上集中後
    - 要求**委外廠商、納入合約**
    - 提供演練紀錄
    - 資料回復驗證

- **每年至少Run一次**

備份

備份種類

- **完整備份**（Full Backup）：
  即把硬碟或資料庫內的所有檔案、資料夾或資料作完整的複製
- **增量備份**（Incremental Backup）：
  指對上一次**完整備份或增量備份**後更新的資料進行備份
- **差異備份**（Differential Backup）：
  差異備份提供執行**完整備份**後變更的檔案的備份

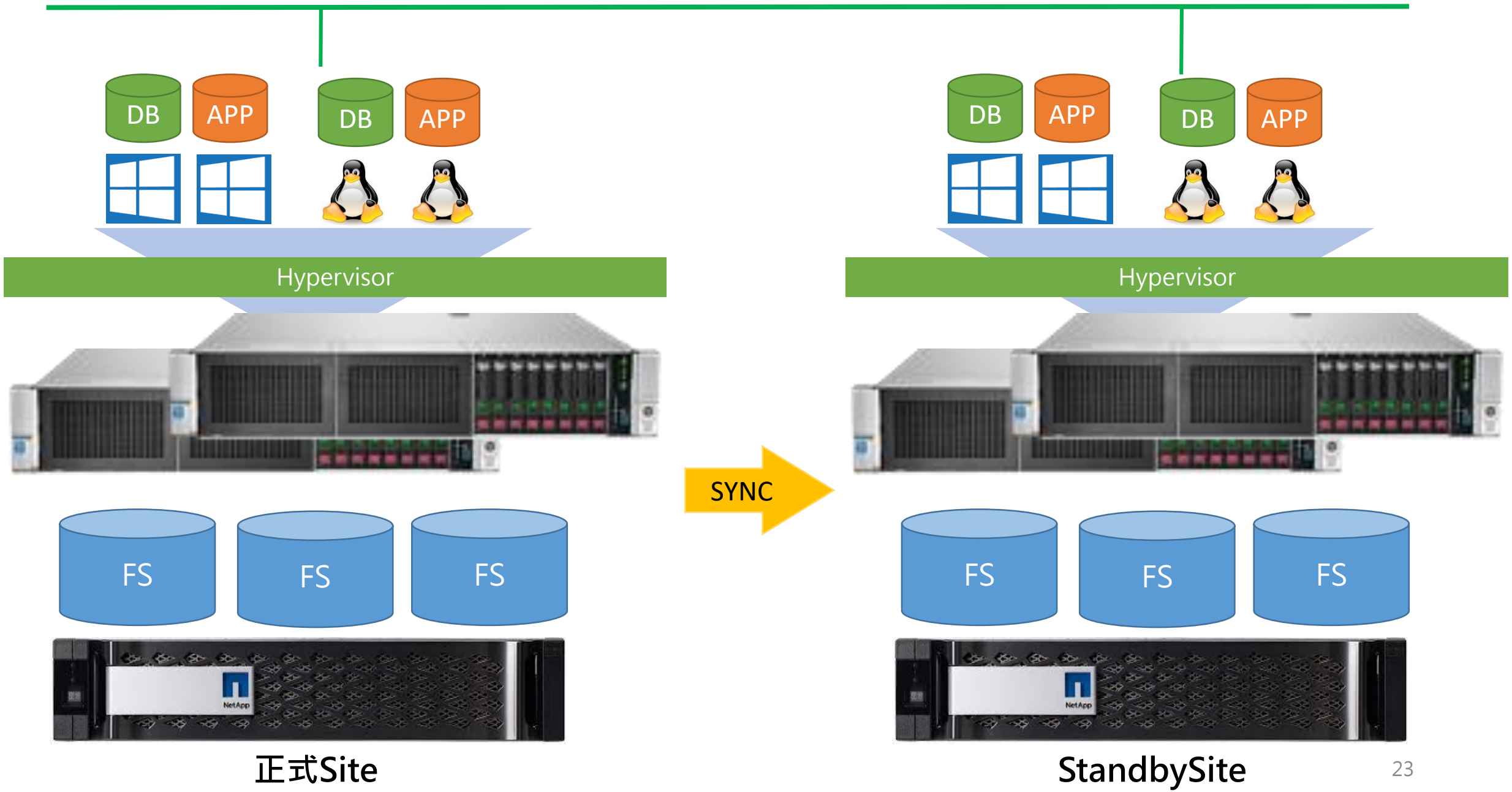
- **冷備份**（Cold Backup）：系統處於停機或維護狀態下的備份。這種情況下，備份的資料與系統中此時段的資料完全一致。
- **熱備份**（Hot Backup）：系統處於正常運轉狀態下的備份。這種情況下，由於系統中的資料可能隨時在更新，備份的資料相對於系統的真實資料可有一定滯後。
- **溫備份**（Warm Backup）：將備份系統已安裝組態成與當前使用的系統相同或相似的系統和網路執行環境，安裝了應用系統，定期備份資料。一旦發生災難，(1)直接使用定期備份資料，手工逐筆或自動批次追補孤立資料或(2)將終端使用者透過通訊線路切換到備份系統，恢復業務執行。

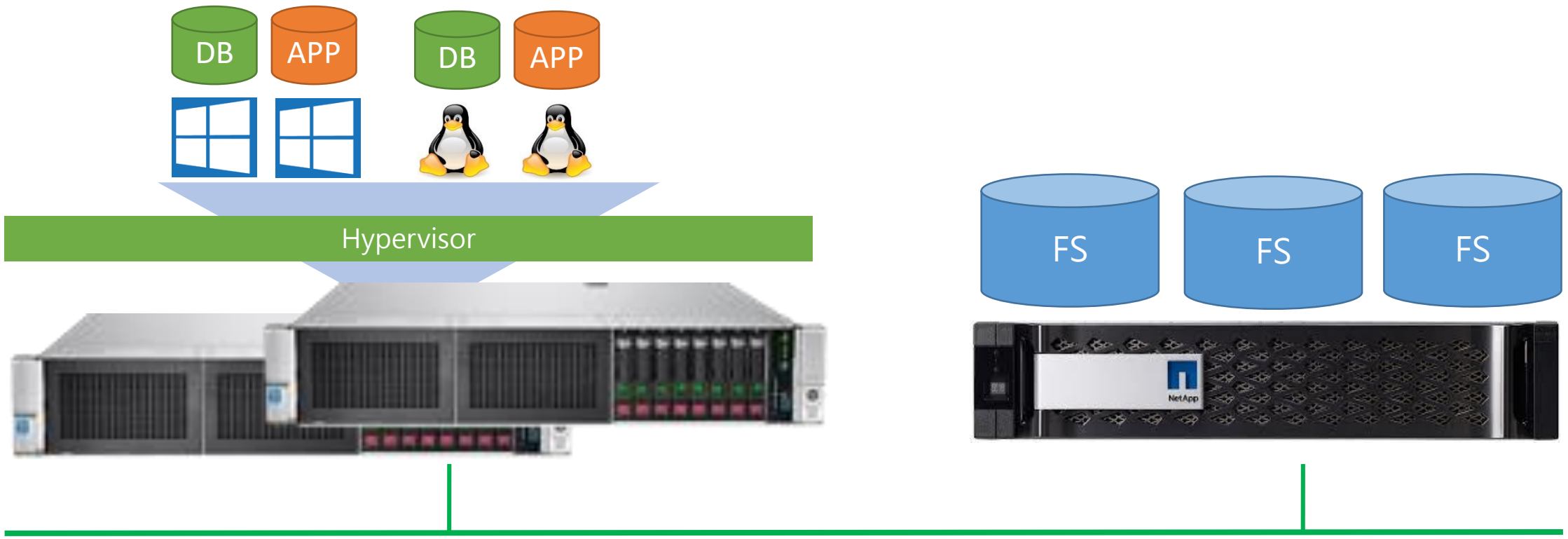
備份類型

- **線上備份**（On-line Backup）：需要及時還原的資料可以採用這總類型的備份，可以使用磁碟陣列、儲存區域網路、網路附加儲存或者是網路硬碟來保護資料安全。

- **離線備份**（Off-line Backup）：離線備份使用可離線媒體來備份，磁帶、光碟或是硬碟盒備份完成後離開備份媒體。

備份作業經驗分享


DB
APP
DB
APP
DB
APP
DB
APP
Hypervisor
Hypervisor
SYNC
FS
FS
FS
FS
FS
FS
正式Site
StandbySite


DB
APP
DB
APP
Hypervisor
FS
FS
FS
NetApp

目前的作法

- 現況：

主要校務系統均虛擬化

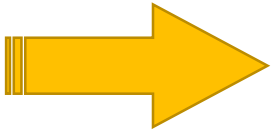
- 複合式備份
  - +1的備份
- 異地備份
- 雲端備份
  - 壓縮、加密

類型	方式		週期
系統	Snapshot，匯出映像檔	每月完整備份	每月
程式碼	資料同步，壓縮備份	每月完整備份+每日差異備份	8個工作小時/24小時
檔案	資料同步，壓所備份	• 每日同步資料 • 同步後的資料：每月完整備份+每日差異備份	8個工作小時/24小時
資料庫	資料庫備份，複製到外部儲存	每日完整備份/每六小時差異備份	每六小時
網路設定	資料匯出	不定期	異動前或後
		每日	8個工作小時/24小時

或採用多版次同步方式
如：以一週為周期
保留七個同步版次

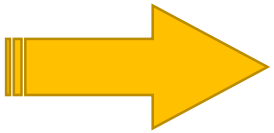
系統備份

- 實體主機：
  - 磁碟系統備份工具
  - 第三方工具軟體
    - Ghost、Arconis、Veem、Nokivo….



- 全系統備份
- 快速還原

- 虛擬主機：
  - **VM工具、功能，快照**
  - **磁碟系統備份工具**
  - 第三方工具軟體
    - Arconis、Veem、Nokivo….



- 全系統備份
- 快速還原
- **快照匯出**

Hypervisor Crash!!

資料庫備份

- 資料庫系統工具
  - MS-SQL
  - MySql、MariaDB
- 第三方工具軟體
  - Arconis、Veem、Nokivo….

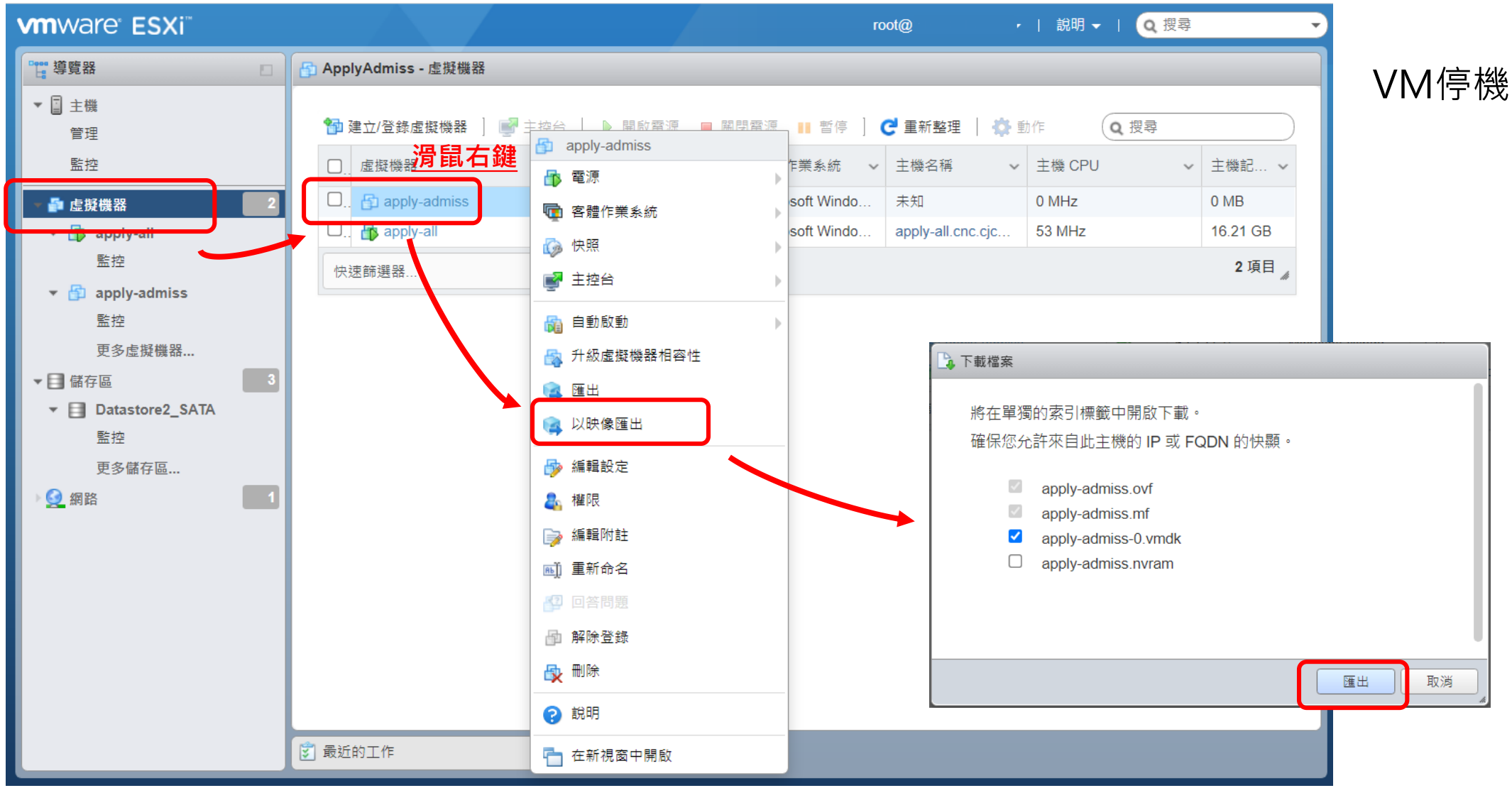
檔案系統備份

- 磁碟系統備份工具
- 第三方工具軟體

注意與提醒

- 磁碟系統備份
  - 硬體的設定?Raid5/6、還原模式?
  - 異地備份?
- 資料庫系統工具
  - 異地備份
- 檔案系統備份
  - 數量大、耗時
  - 耗費IO
  - 影響系統運作~

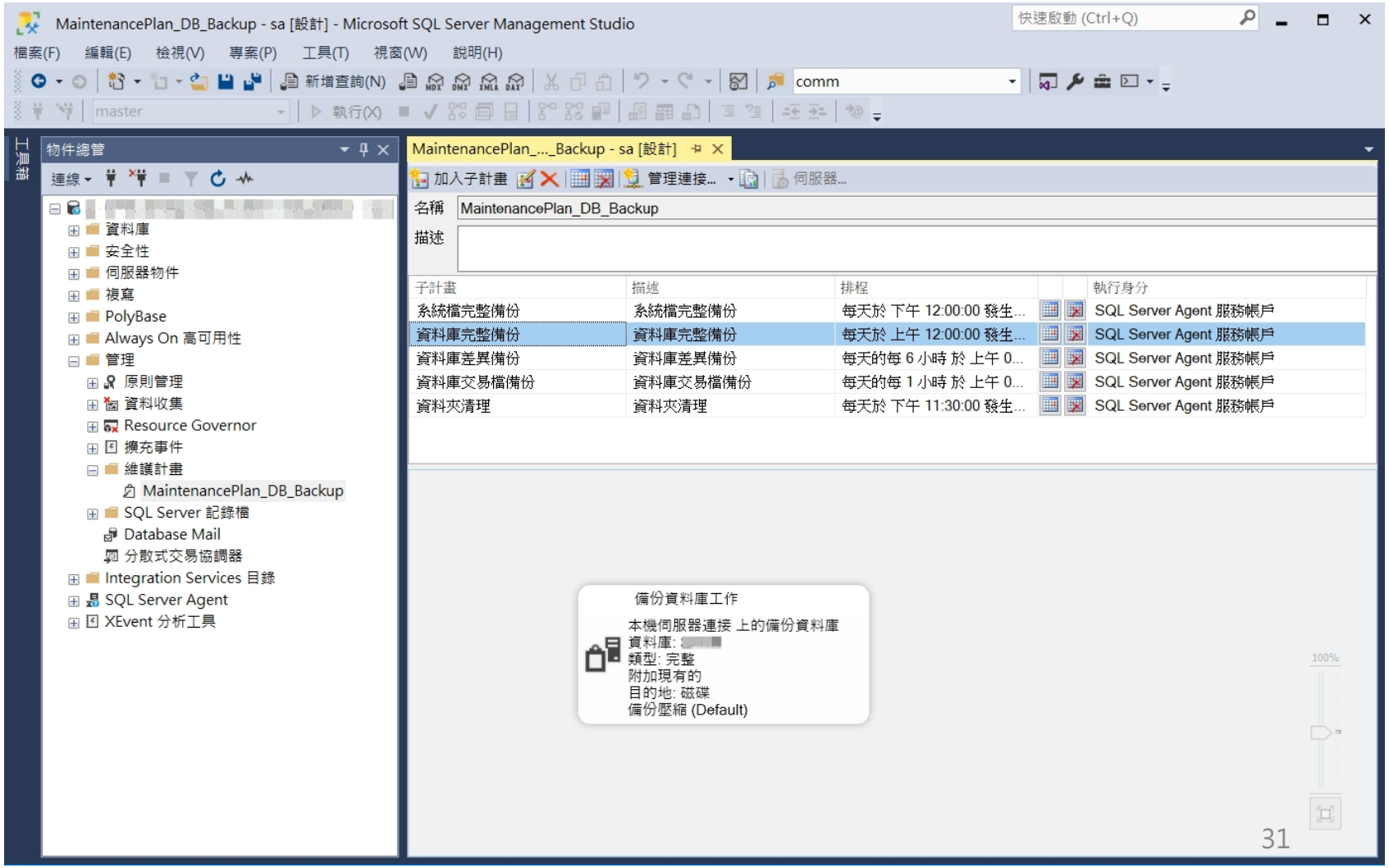
備份實務-VMimage



VM停機狀態下執行

備份實務-MS-SQL

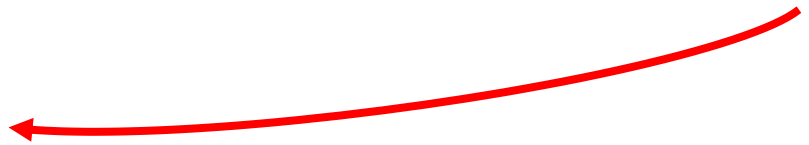
- 完整+差異
- 六小時備份一次
- **定時利用工具軟體複製備份檔案至外部儲存裝置**



備份實務-MySQL

- 完整
- 建議在離峰執行
  - mysqldump -uusername –pXXXXXXXX DB_NAME > all.sql
  - Mysqlhotcopy –u username –p XXXXXXXX DB_NAME 目標目錄

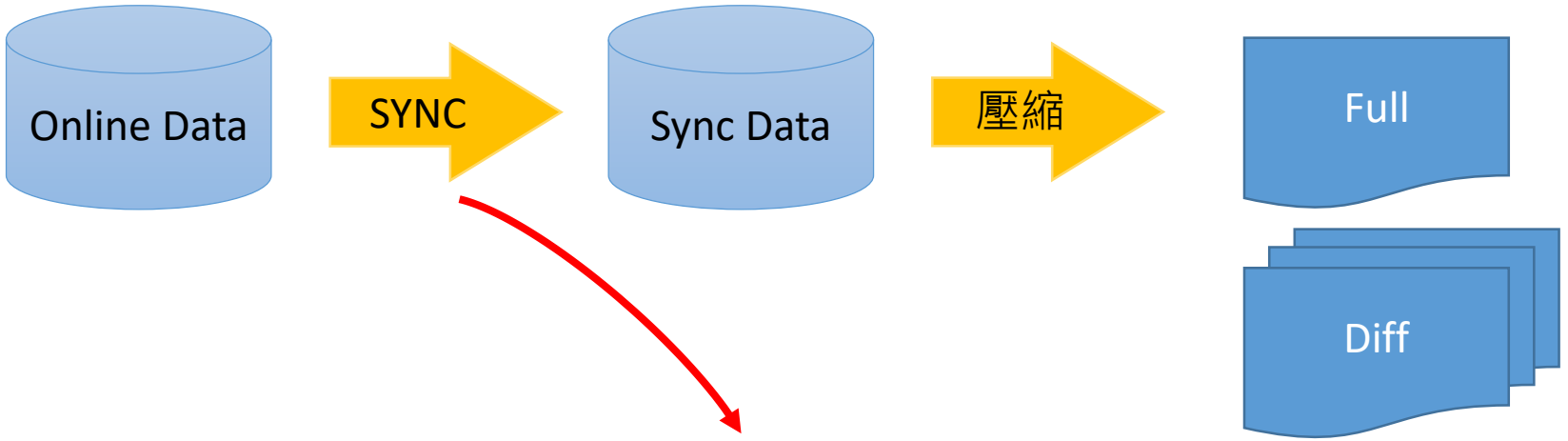
目標目錄建議在不同硬碟



慘痛經驗

- 2008年，**採用S牌備份軟體備份資料庫檔案**
- 某次系統還原測試，發現所有資料都無法還原~~~
- 從此以後
  - 利用MS-SQL內建功能備份

備份實務-檔案系統



- 注意目錄結構
- 小檔案數量大、耗時
- 耗費IO
- 影響系統運作~

Linux檔案系統備份常用指令

- rsync
  - --bwlimit限制流量
  - --delete同步刪除
  - --exclude排除向
- 方法：利用script拆解目錄

```
cd /source_data
for dir1 in $(ls)
do
  mkdir –p /backup
  rsync -avug --bwlimit=1000 --delete --progress $dir1 /backup
done
```

#tar –zcvf /source_data /backup/backupfile.tgz

#zip –P password –D -9 backupfie.zip backupfie

營運持續演練的執行

- 用意
  - 驗證回復計畫
  - 驗證RPO、RTO有效
  - 驗證**備份資料**可用
- 週期
- 測試哪一份備份資料?
  - 異地的那一份~~~

營運持續演練回復測試驗證

- 系統功能驗證
- 資料庫資料驗證
  - 資料庫工具抽驗
- 檔案系統驗證
  - 檔案抽驗

- Microsoft SQL Server Management Studio
- phpmysqladmin
- HeidiSQL

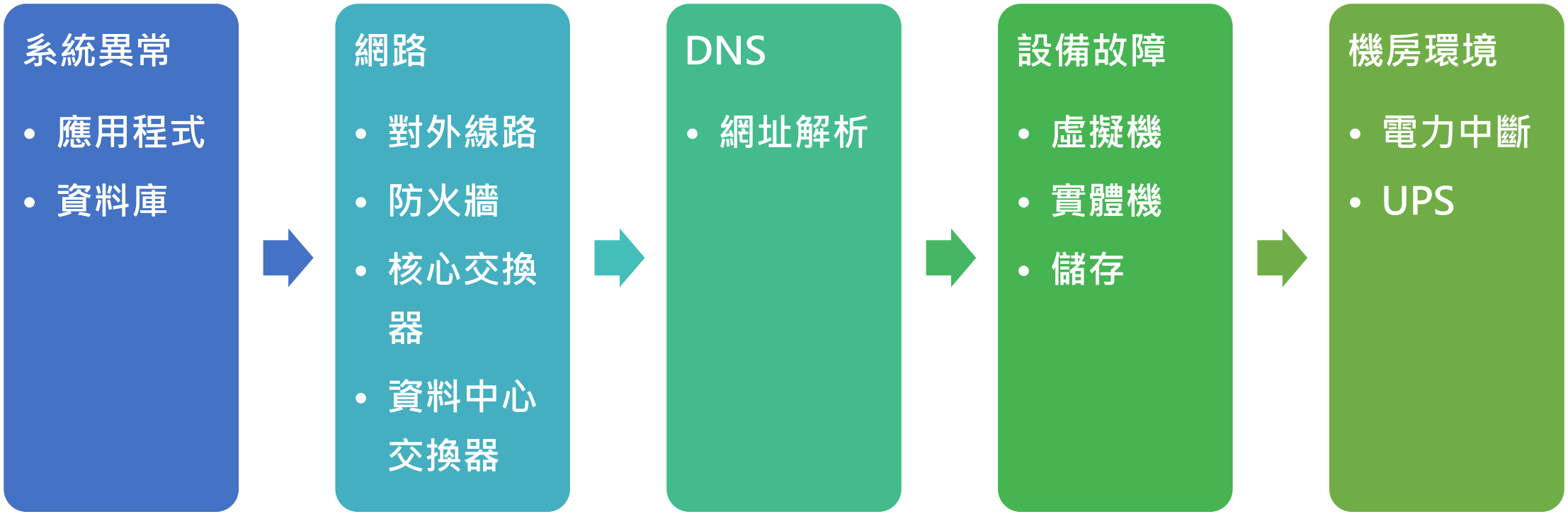
營運持續演練**紀錄**的用意

- 紀錄時間
- 截圖

- 計時開始：演練開始
- 關鍵步驟的花費時間
- 驗證RTO有效性

- 紀錄
  - 關鍵步驟
  - 關鍵指令
  - Step by Step
- **建立緊急事件處理的SOP**

關鍵業務


系統異常
• 應用程式
• 資料庫
網路
• 對外線路
• 防火牆
• 核心交換器
• 資料中心交換器
DNS
• 網址解析
設備故障
• 虛擬機
• 實體機
• 儲存
機房環境
• 電力中斷
• UPS

情境題

學校官網圖案遭到置換，需於10分鐘內更換為靜態維護頁面

- 主關機關規定：
  - 於發現置換後**10分鐘內**更換成靜態維護頁面。
  - 於**知悉確認為資安事件後一小時內**依據相關流程通報。
    - 臺灣學術網路各級學校資通安全通報應變作業程序
  - 國教署**委辦資訊系統30分鐘內**，通報委託此業務組室轉秘書室

演練腳本

此腳本不包含系統重建、證據鑑識

時間	動作	參與人員	地點	備註
T	• 演練開始			
T 至 T+2分鐘	• 發現學校官網圖案遭到置換	系統管理人員	辦公室	
T+2分鐘 至 T+5分鐘	• 確認學校官網圖案遭到置換之確切狀況通報主管	系統管理人員	辦公室	
T+5分鐘 至 T+10分鐘	• 執行資安事件通報作業	系統管理人員	辦公室	
	• 切換學校官網為【維護中】之靜態網頁 • 建議採用： 1. DNS 解析導向新主機 2. http redirect	系統管理人員	辦公室/機房	
T+10分鐘 至 T+15分鐘	• 系統連線測試，確認畫面導向	系統管理人員	辦公室/機房	
T+15分鐘 至 T+30分鐘	• 遭入侵系統封存(證據留存)	系統管理人員	辦公室/機房	
T+30分鐘 至 T+50分鐘	• 產出「異常事件紀錄表」or「安全事件處理紀錄表」。 • 回報主管事件處理完畢。	系統管理人員	辦公室	

演練紀錄

- SOP
- 關鍵指令
- 截圖

Q and A

Thank You~~