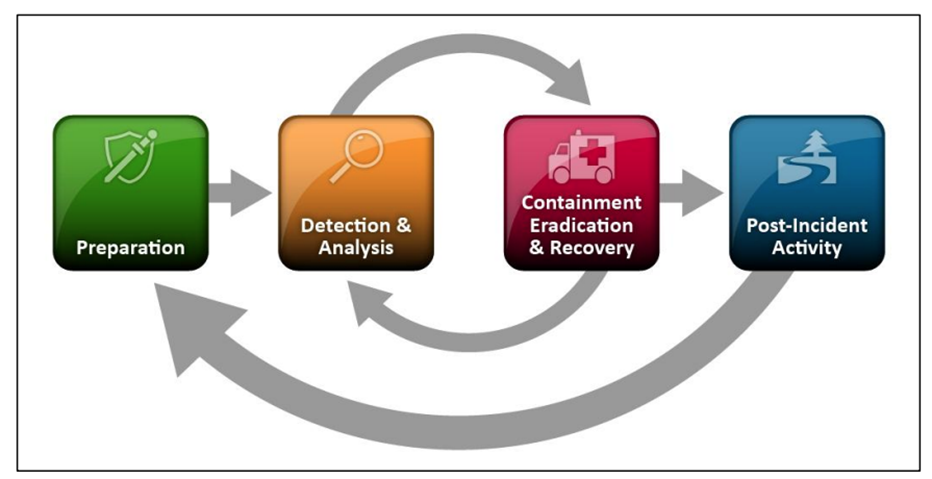
事故處理流程

**資訊安全日誌、事件、事故的差異**

* 日誌 (Log)
  + 只是如實記錄所有系統活動，人、事、時、地、物。
  + 範例：「使用者A在9:00-9:15嘗試登入5次失敗」
* 資訊安全事件 (Information Security Event)
  + 需要資安人員定義事件指標與判斷的異常現象。
  + 範例：
    - 事件指標：15分鐘內密碼錯誤5次。
    - 需要判斷：是員工忘記密碼？還是遭受攻擊？
    - 不處理的話有可能會變成事故。
* 資訊安全事故 (Information Security Incident)
  + 確認造成組織傷害的安全事件。
  + 範例：確認是駭客嘗試破解密碼並成功入侵系統，或發現敏感資料已遭未授權存取。
  + 須依組織政策啟動正式事故應變程序。



(資料來源：網際網路)

**NIST 800-61 Rev. 2 電腦安全事件處理指南**

* 準備 (Preparation)
  + **制定應變計畫與通報機制：**撰寫明確事故情境與處置步驟，確立決策權責。
  + **組建並訓練應變團隊：**選派跨部門專家定期演練，確保熟悉程序與工具。
  + **確保系統與工具就緒：**預先部署防護、監控與取證工具，降低事故爆發風險。
  + **建立證據管理與溝通流程 (Chain of Custody)：**設計內外部溝通管道，同時訂定證據收集與保存規範。
* 偵測與分析 (Detection and Analysis)
  + **監控與警報分類：**持續監測系統並快速區分真實威脅與誤報，避免資源浪費。
  + **確認事故種類與範圍：**判斷事故類型與受影響系統，建立初步處理優先順序。
  + **評估業務與運營影響：**評估對財務、營運與商譽的潛在損害，調整應變策略。
  + **深入調查與數位鑑識 (Digital Forensics)：**彙整線索、建立時間軸，保存關鍵日誌與數位證據。
* 遏制、根除與復原 (Containment, Eradication, and Recovery)
  + **實施遏制措施：**立即隔離受影響系統或網段，防止威脅擴散。
  + **雙軌工作分組：**一組執行遏制和復原，另一組負責持續收集與保全證據。
  + **根除威脅：**移除惡意程式、修補漏洞，消除後門與潛在的再入侵途徑。
  + **系統復原與驗證：**從乾淨備份還原系統，進行安全確認後才恢復正常運作。
* 事後檢討(Post-Incident Activity)
  + **完整事故報告與溝通：**記錄事故過程與影響，向內外部利害關係人提供資訊。
  + **法律與合規處理：**整理保全的證據鏈，準備可能的法律訴訟、監管報告或保險索賠。
  + **根因分析與防護改進(Root Cause Analysis)：**找出根本原因，修訂應變流程與強化系統防護措施。
  + **經驗傳承與持續監控(Lessons Learned)：**將學到的教訓納入內部知識庫，並持續追蹤新威脅情資。

# **勒索病毒事故應變流程案例**

## **情境背景：**

某公司週一早上9點，多位員工回報無法存取重要文件，部分檔案出現「.encrypted」副檔名，並發現勒索訊息要求支付5比特幣以取回解密金鑰。

## **1. 準備 (Preparation)**

* **制定應變計畫與通報機制**：根據預先制定的勒索軟體應變計畫，IT主管立即通知資安長並啟動資安事故應變小組，同時依通報流程向執行長報告情況。
* **組建並訓練應變團隊**：資安小組迅速集結曾進行過勒索軟體演練的跨部門專家，包括資安、IT、法務與公關人員，各自依角色分工。其中兩名IT安全工程師受過第一線鑑識應變(First Responder)訓練，能進行初步證據保全。
* **確保系統與工具就緒**：應變團隊確認備援系統正常，並啟用資安工具進行調查，包括EDR、SIEM與網路監控系統。同時準備初步鑑識工具包，包含可寫保護設備與記憶體取證工具。
* **建立證據管理與溝通流程 (Chain of Custody)**：指派數位鑑識專家負責蒐證，使用預先準備的證據收集表格記錄所有發現，並建立內部通訊群組確保資訊即時流通。同時聯繫合約中的專業數位鑑識公司進行支援。

## **2. 偵測與分析 (Detection and Analysis)**

* **監控與警報分類**：分析EDR警報發現可疑活動始於週日晚間11點，確認為真實威脅而非誤報。
* **確認事故種類與範圍**：技術團隊確認為Lockbit 3.0勒索軟體，已加密財務部門與行銷部門共35台主機，但核心生產系統目前未受影響。
* **評估業務與運營影響**：業務分析顯示財務系統無法正常運作，影響員工工資處理與月底報表產出，預估每天停機損失約10萬元，同時評估客戶數據是否外洩。
* **深入調查與數位鑑識 (Digital Forensics)**：受過第一線鑑識應變訓練的內部人員立即保全受影響系統的揮發性證據，包括記憶體映像與網路連線狀態，同時凍結關鍵系統變更。隨後到場的專業鑑識公司接手這些初步證據，進一步分析Windows事件日誌與防火牆記錄，確認攻擊者透過公司對外開放的3389端口（RDP）成功暴力破解弱密碼一般使用者帳號。日誌顯示攻擊源IP有多次失敗登入紀錄，最終於週日晚間成功登入。進一步調查發現攻擊者登入後利用本地提權漏洞（CVE-2021-34527，PrintNightmare漏洞）獲取系統管理員權限，接著使用盜取的憑證進行橫向移動，最終部署勒索軟體。

## **3. 遏制、根除與復原 (Containment, Eradication, and Recovery)**

* **實施遏制措施**：基於確認的攻擊途徑，立即隔離受感染網段，關閉所有對外RDP連線，同時更改全公司密碼並啟用多因素認證。
* **雙軌工作分組**：完全分離兩個團隊工作 - 應變復原團隊專注於遏制與系統恢復；同時鑑識團隊（包含內部第一線鑑識應變人員與外部專業鑑識公司）專責證據保全與分析。內部第一線鑑識應變人員在專業鑑識公司到場前負責初步證據收集與保全，確保關鍵揮發性證據不被破壞，並維護完整的證據保管鏈 (Chain of Custody)。兩團隊透過事故指揮中心協調，避免復原行動破壞重要證據。
* **根除威脅**：清除識別出的惡意程式，修補PrintNightmare漏洞（CVE-2021-34527）與其他系統漏洞，重新設計遠端存取架構改用VPN加雙因素認證，並在所有端點更新EDR病毒碼。
* **系統復原與驗證**：從上週五的備份還原財務系統，在隔離環境中進行安全掃描確認無惡意程式後，逐步恢復業務系統運作。

## **4. 事後檢討 (Post-Incident Activity)**

* **完整事故報告與溝通**：綜合內部調查與外部鑑識公司的報告，撰寫詳細事故報告，向管理層說明事故經過，並依法規要求通知個資主管機關與受影響客戶。
* **法律與合規處理**：法務團隊評估事件法律風險，將收集的證據交予執法單位，並準備保險理賠所需文件。外部鑑識公司的專業報告成為保險理賠與潛在法律訴訟的重要佐證。
* **根因分析與防護改進 (Root Cause Analysis)：**分析顯示事件根本原因包括：
  1. 暴露在公網的RDP服務未實施適當防護措施（如IP白名單、網路層防火牆）
  2. 一般使用者帳號使用弱密碼，易遭暴力破解
  3. 系統存在未修補的PrintNightmare本地提權漏洞（CVE-2021-34527）
  4. SIEM系統未配置適當的RDP暴力破解與異常權限提升偵測規則
  + 立即制定改善計畫包括實施跳板機制、嚴格的密碼政策、建立完善的漏洞管理與修補流程，以及優化SIEM監控機制。
* **經驗傳承與持續監控 (Lessons Learned)**：將此次事件經驗納入教育訓練課程，強化員工資安意識。增加內部第一線鑑識應變的培訓與認證，確保關鍵證據能在第一時間被正確保全。重新審視與調整SIEM偵測規則，特別是針對RDP暴力破解嘗試及異常權限提升行為設定更低的閾值與即時警報。同時實施定期弱點掃描、暴露面評估，並定期檢視SIEM的偵測有效性。

**考古題：**

10.據NISTSP800系列標準，關於災難復原計畫(DisasterRecoveryPlan，DRP)、業務持續性計畫(BusinessContinuityPlan，BCP)和資訊系統應急準備計畫(InformationSystemContingencyPlan，ISCP)的關聯性，下列何項描述正確？

(A) 災難復原計畫(DRP)專注於資訊技術系統的恢復，而業務持續性計畫(BCP)和資訊系統應急準備計畫(ISCP)則專注於組織的整體運營恢復

(B) 資訊系統應急準備計畫(ISCP)涵蓋整個組織的業務和資訊系統恢復策略，而災難復原計畫(DRP)和業務持續性計畫(BCP)則關注於特定技術解決方案

(C) 業務持續性計畫(BCP)專注於資訊技術系統的恢復，而災難復原計畫(DRP)和資訊系統應急準備計畫(ISCP)則專注於組織的整體運營恢復

(D) 災難復原計畫(DRP)專注於資訊技術系統的恢復，業務持續性計畫(BCP)涵蓋組織整體的業務運營持續性，而資訊系統應急準備計畫(ISCP)則專注於特定資訊系統的應急反應

規劃 114-1 答案D

(BCP → 整體營運業務

DRP → 機房、硬體、網路等資訊基礎設施恢復

ISCP → 特定應用系統（如核心帳戶系統）的恢復細節)

42. 依據SP 800-61 Rev. 2 - Computer Security Incident Handling Guide文件對於事故回應生命週期（Incident Response Life Cycle）之敘述，下列何者錯誤？

(A) 準備（Preparation）

(B) 偵測與分析（Detection and Analysis）

(C) 封鎖、根除與復原（Containment, Eradication and Recovery）

(D) 備份（Backup）

管理 113-2 答案D

(備份非事故回應生命週期，應該是事後檢討)

43. 關於一般資安事件與重大資安事故的描述，下列何者較「不」適當？

(A) 事件處理時間超過規定時，會升級為事故

(B) 影響資安指標達成之因素或事項者，依其嚴重性評估不會被判定為事件

(C) 一般資安事件與重大資安事故可依照對公司組織的影響程度作為區分

(D) 重要資訊設備失效，通常會歸類為重大資安事故

管理 113-2 答案B

(任何可能影響資安指標（例如機密性、完整性、可用性）的因素或事項，無論其嚴重性，都應該被視為潛在的資安事件，並進行評估和處理。即使是看似輕微的問題，如果不加以處理，也可能升級為更嚴重的問題，或被攻擊者利用。因此，這選項的描述是錯誤的。)

8. 企業資安事件類型「不」包含下列何項？

(A) 機房漏水

(B) 備用發電機啟動故障

(C) 外部廠商發生資料外洩

(D) 私人手機遺失 (私人手機遺失，除非該手機內存有企業敏感資料，且未受適當保護（例如：未加密、未使用強密碼），或者該手機被用來進行雙重驗證且無其他備用驗證方式，否則一般不被視為企業資安事件。這屬於個人資安事件)

防護 113-1 答案D

9. 進行資安事件處置時，下列做法何者錯誤？

(A) 將漏洞修補以防止再發生

(B) 原始稽核紀錄可以刪除 (這是錯誤的做法。原始稽核紀錄是調查資安事件的重要證據，應該妥善保存，不能隨意刪除。稽核紀錄可以幫助還原事件發生的過程，找出事件的根本原因，以及評估損害的範圍等)

(C) 確認事件根因是必要的

(D) 可以委託外部專業廠商進行

防護 113-1 答案B

12. 事故回應（Incent Response IR）的處理流程中，依據 NIST SP800-61 r2在隔離、清除和恢復階段中，下列何項是最佳處

理方案？

(A) 立即更新安全政策

(B) 隔離受影響系統 (隔離是最重要的，類似失火先救火)

(C) 開始法律行動

(D) 立即針對員工進行安全培訓

防護 113-1 答案B

21. 廠商攜帶設備至機關進行維護作業，機關允許該設備連線至機房網路，待設備接上網路並操作一段時間後，監控中心即發現符合特定惡意程式行為之連線。下列建議之防護措施何者最「不」合適？

(A) 機關收到監控中心異常通知後，即時將廠商設備斷網

(B) 攜帶之設備或工具應確保安全無虞，方可連線至機關內部網路

(C) 廠商應恪守機關資通安全政策及委外廠商管理相關規範要求

(D) 須等相關工作結束後，再關閉網路連線 (是不合適的措施。發現異常行為後，應該立即採取措施阻止進一步的損害，而不是等待工作結束。等待工作結束可能會導致惡意程式擴散、資料外洩等嚴重後果)

防護 113-1 答案D

41. 當資訊安全事故發生時，下列敘述何者正確？

(A) 資訊安全事故的發生，最好將細節全部記錄下來，以做日後分析使用

(B) 因為是資訊安全事故，僅對內部告知，細節要求不需告知與資訊處理相關的供應商

(C) 資訊安全事故發生如果無法找到根本原因，可以先予以結案

(D) 因為成本資源的限制，增加此資訊安全事故不再重複發生的控制措施，可於日後再實施

管理 113-1 答案A

(B錯在應通知相關受影響供應商

C錯在未找到根本原因不應結案

D錯在應立即實施預防措施而非延後)

45. 資安事故的通報程序「不」包括下列何項？

(A) 向連絡窗口通報

(B) 記錄相關細節

(C) 向警察機關報案

(D) 產生事故結案報告

管理 113-1 答案D

(通報程序通常不包含結案報告，但是C選項需視事故性質而定（如涉及犯罪、個資外洩等）)

42. 關於資訊安全事故處理的相關敘述，下列何者較正確？

(A) 發生資訊安全事故時先予以處理，後續再蒐集相關資料 (應該要同時蒐集證據找到根因)

(B) 事故發生後， 應針對事故留存相關紀錄並檢討與改進

(C) 發生資訊安全事故時先予以處理，處理完後再通報相關主管機關 (資通安全管理法要求知悉後一小時內通報主管機關)

(D) 日常發生與資訊安全相關的議題，盡量以事件處理不要提升至事故等級 (如果是已經發生損失還是要提升到事故等級)

管理 112-2 答案B

(事故後應保留完整紀錄以供檢討改進，避免類似事故再次發生，並依此更新安全政策和措施，故選B)

44. 試問有關資訊安全事件（Information Security Event）與資訊

安全事故（Information Security Incident）之敘述，下列何者錯誤？

(A) 資訊安全事件是系統或網路中任何可觀察到的現象或徵兆，可以無須理會

(B) 防毒軟體攔截到一個病毒係屬於資訊安全事件

(C) 資訊安全事故已經對組織造成影響

(D) 駭客入侵組織內部網路竊取資料係屬資訊安全事故

管理 112-2 答案A

(資通安全事件是系統或網路中任何可觀察到的現象或徵兆，不處理的話有可能會變成事故)

44.資訊安全事故發生後，證據蒐集的相關敘述，下列何者較正確？

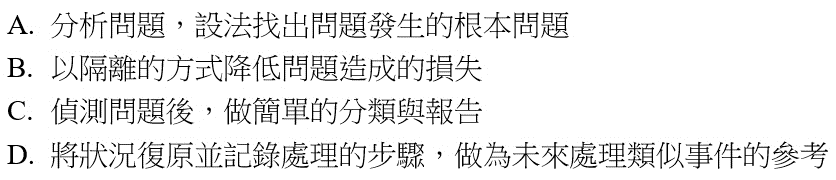
(A) 組織可考量與數位證據控管有關的工具導入，以確保對數位證據的有效保存

(B) 於資訊安全事故發生後，若需要針對證據予以鑑識，一旦超過組織之權限，即無法提供使用 (超出權限時可尋求外部專業協助)

(C) 若資訊安全事故涉及法律議題相關，證據保存存在困難程度，所以無法實施控管 (在涉及法律時更應嚴格保存證據，例如證據監管鏈)

(D) 資訊安全事故的發生會揭露內部的問題，所以不適合文件化太過詳細 (事故紀錄應盡可能詳細完整，重點在根因分析，避免下次再度發生)

管理 112-1 答案A

45. 如附圖所示，資訊安全事件處理的正確步驟順序為下列何項？

(A) ABCD

(B) ACBD

(C) CBAD

(D) DBCA

管理 112-1 答案C

(資訊安全事件處理的正確順序應是：

1. C-先偵測並快速分類報告
2. B-採取隔離措施降低損害
3. A-分析找出根本原因
4. D-記錄處理步驟供未來參考

所以選C(CBAD)，這樣的順序能確保先快速應變、控制損害，再深 入分析和總結經驗)

46. 關於事件應變，下列敘述何者較正確？

(A) 為求時效，一旦找到受感染主機應立即進行證據採樣 (事件應變的首要步驟是隔離受感染主機，防止威脅擴散)

(B) 資料收集時，應著重在相關人員的口述資料 (技術證據如日誌、網路流量、磁碟映像才是分析攻擊的關鍵)

(C) 主機與網路證據為常見搜集標的

(D) 鑑識分析之最終目的為反擊攻擊來源 (鑑識分析的主要目標是釐清事件原因、遏制威脅、恢復系統，並為法律行動提供證據)

管理 111-1 答案C

營運持續和備援

**營運持續相關名詞 (參考NIST 800-34, Rev 1)**

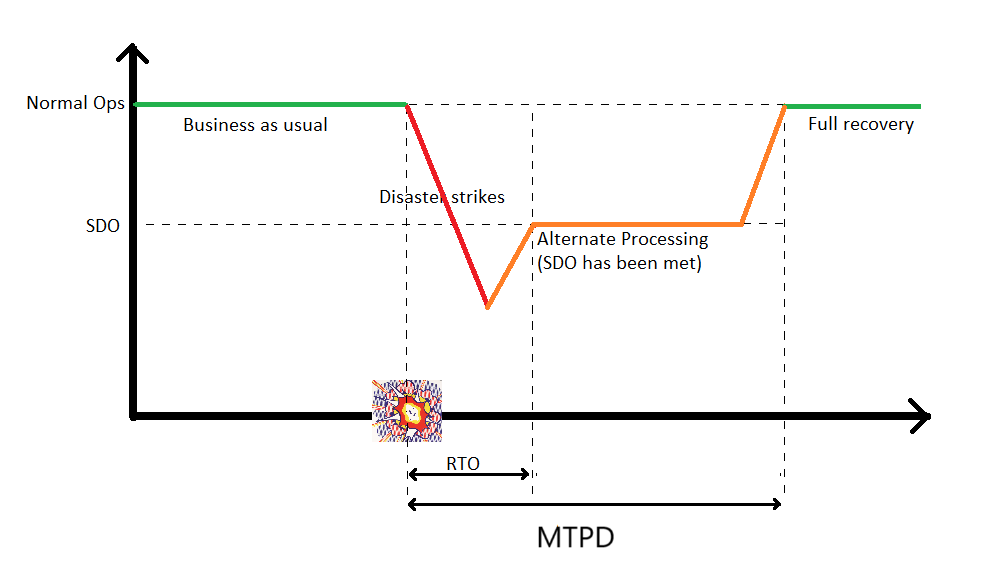
* BCP (Business Continuity Plan，業務持續計畫)：
  + 目的：確保企業在災難或意外發生時，關鍵業務運作仍能持續或快速恢復正常運作。
  + 內容重點：企業的核心業務運作、關鍵流程、資源調度、人員管理、替代作業地點、臨時替代方案。
  + 特點：全面性計畫，涵蓋企業整體營運，著重事故後業務的持續性。
* DRP (Disaster Recovery Plan，災難復原計畫)：
* 目的：在IT系統或資料中心發生重大災難後，快速恢復資訊系統的運作能力。
* 內容重點：系統備份與恢復程序、資料重建程序、替代設備啟動、異地備援中心（Hot site、Cold site）的啟動程序。
* 特點：偏重於資訊科技層面、機房設施、系統環境等的技術性恢復。
* ISCP (Information System Contingency Plan，資訊系統應變計畫)：
* 目的：當資訊系統發生故障、網路攻擊或異常狀況時，提供具體且明確的應變步驟，快速恢復特定系統運作。
* 內容重點：特定系統的備援措施、系統降級模式、異常診斷、應急處理程序與驗證。
* 特點：聚焦於特定的資訊系統，較DRP更為具體且精細。

**銀行業務營運持續案例**

* BCP（分行營運持續）
  + 當重大事故發生（如系統當機、資安事件）時，分行可能改為手動模式服務客戶，如：
  + 例如：
    - 臨時改為手動登記帳戶往來。
    - 以書面作業取代電子作業。
    - 緊急人員調度、通訊與聯絡方式。
* DRP（備援機房啟動）
  + 若需切換至備援機房運作，將參考DRP執行，例如：
    - 備援機房的地點及緊急聯絡人。
    - 備援機房基礎設施（網路、電力、空調等）啟動步驟。
    - 資訊系統硬體設備啟動順序及網路架構調整的詳細指引。
* ISCP（核心帳戶系統恢復）
  + 若核心帳戶系統出現異常或需要緊急維護，將依照ISCP執行，例如：
    - 帳戶系統的備份資料庫還原程序。
    - 異常診斷與問題排除步驟。
    - 系統降級模式（degraded mode）的啟動流程。
    - 完成復原後，進行系統驗證與重新上線確認程序。
  + ISCP的獨立使用情境補充：ISCP不一定僅於災難（如切換DRP備援）發生時使用，更常用於規模較小、針對單一系統的緊急狀況，例如：
    - 單一硬碟損壞。
    - 主機或伺服器故障。
    - 特定應用系統（例如網銀或帳戶系統）運作異常。

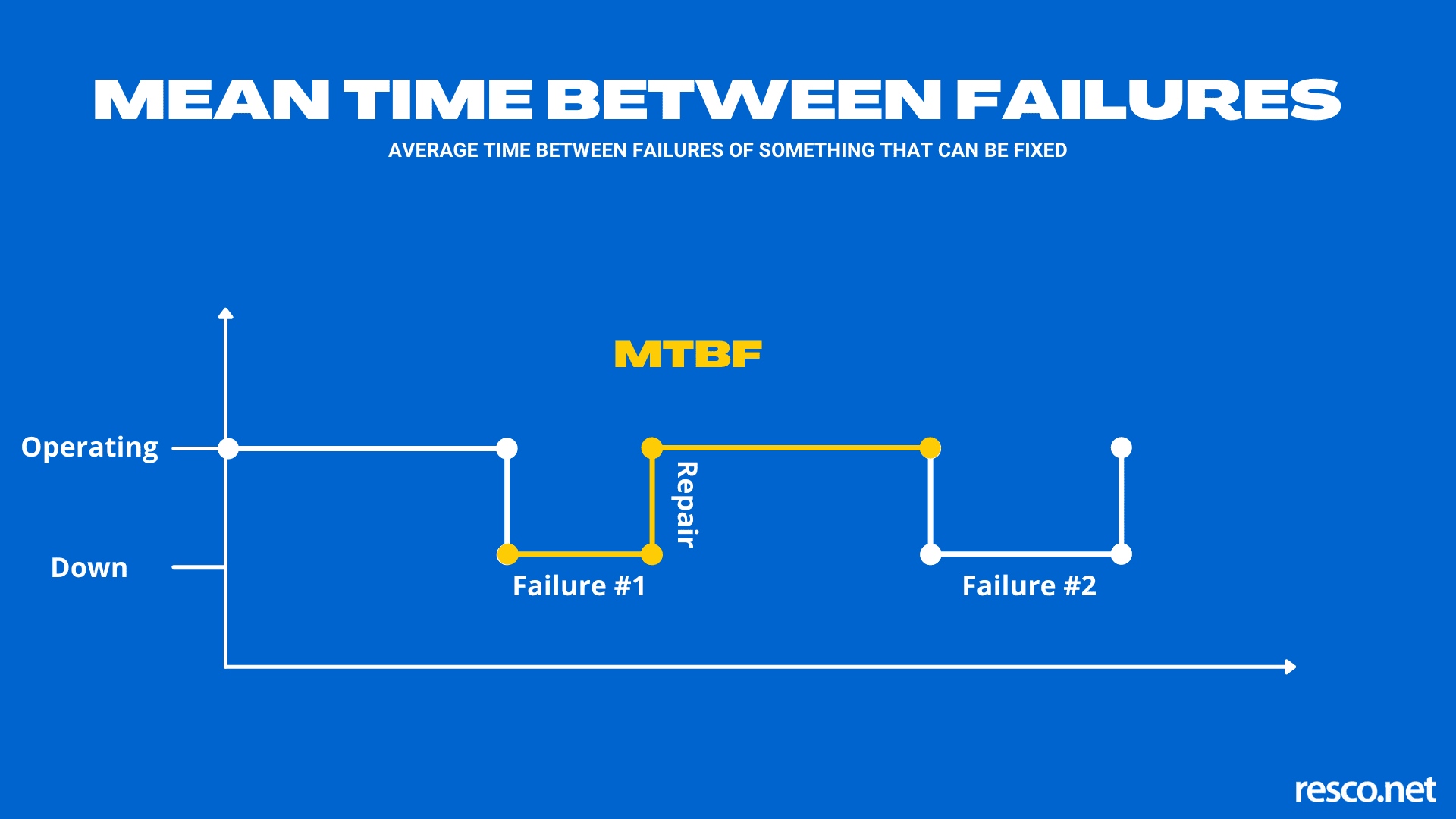
**營運持續關鍵指標**

* BIA (營運衝擊分析)
* 目標：評估災難影響有多大，決定優先恢復順序
* 評估項目：
  + 復原至最低營運程度所需的員工、技能、設施與服務。
  + 災難造成的損害，如：收入損失、附加成本、商譽損失、競爭優勢喪失。
  + 完全復原至原服務水準的所需時間。
  + 服務是否有恢復之相依性。
* RPO (復原點目標)
* 定義：容許丟失多少時間的資料，因此與備份間隔時間相關。
* RTO (復原時間目標)
  + 定義：系統需要多久時間才能恢復到到最低服務水準。
* SDO (最低服務水準)
  + 定義：在RTO時間內必須要達到的最低服務水準，例如60%負載量。
* MTPD 或 MTD (最大可容忍中斷時間)
* 定義：業務最多可以停多久，超過這個時間公司會有重大損失，因此 RTO 必須小於 MTPD 。



(資料來源：網際網路)

* MTTF (Mean Time To Failure) (平均失效時間)
  + 定義： 系統從開始運行到發生失效的平均時間。
  + 重點： 反映系統或設備的可靠性和無故障運行時間。
  + 指標： MTTF 越高，系統越可靠，故障間隔越長。
  + 範例： 伺服器平均運行 50,000 小時後發生故障，則 MTTF 為 50,000 小時。
* MTTR (Mean Time To Recovery) (平均復原時間)
  + 定義：系統從故障發生到完全恢復正常運作所需的平均時間。
  + 重點： 反映故障後的恢復速度和維修效率。
  + 指標： MTTR 越低，系統恢復越快，可用性越高。
  + 範例： 伺服器平均每次故障需 2 小時恢復，則 MTTR 為 2 小時。
* MTBF (Mean Time Between Failures) (平均故障間隔時間）
  + 定義： 可修復系統兩次連續故障之間的平均時間，包含正常運行時間和修復時間。
  + 公式： MTBF = MTTF + MTTR
  + 重點： 評估系統可靠性和可用性的重要指標。
  + 較高的 MTBF 表示系統故障間隔時間較長，但如果 MTTR (平均復原時間) 也較長，則實際可用性不一定較高。需要結合 MTTF 和 MTTR 綜合判斷。
  + 範例：
    - Toyota 汽車: MTTF = 10,000 小時，MTTR = 20 小時，MTBF = 10,020 小時。
    - Tesla 汽車: MTTF = 11,000 小時，MTTR = 2160 小時，MTBF = 13,160 小時。
    - 結論： Tesla 的 MTBF (13,160 小時) 高於 Toyota (10,020 小時)，乍看之下 Tesla 的故障間隔時間更長。然而，在相同的時間週期 (例如 13,160 小時) 內，由於 Tesla 的 MTTR (維修時間) 過長，其可用時間比例 (11,000 小時) 反而低於 Toyota (約 13,133 小時(註1))。 因此，Toyota 的可用性更高。單看 MTTF 會誤以為 Tesla 更可靠，單看 MTBF 會誤以為 Tesla 可用性更高 (因為其數值更大)，需要將 MTBF 放在相同的時間週期下比較，才能得出正確的可用性高低關係。
    - 註1：更詳細的解釋 (基於 13,160 小時的時間週期)：Toyota: 大約可以運行 1.31 個週期 (13,160 / 10,020)，總運行時間約 13,133 小時 (1.31 x 10,000)，總維修時間約 26.2 小時 (1.31 x 20)。Tesla: 可以運行 1 個週期，運行時間 11,000 小時，維修時間 2,160 小時。

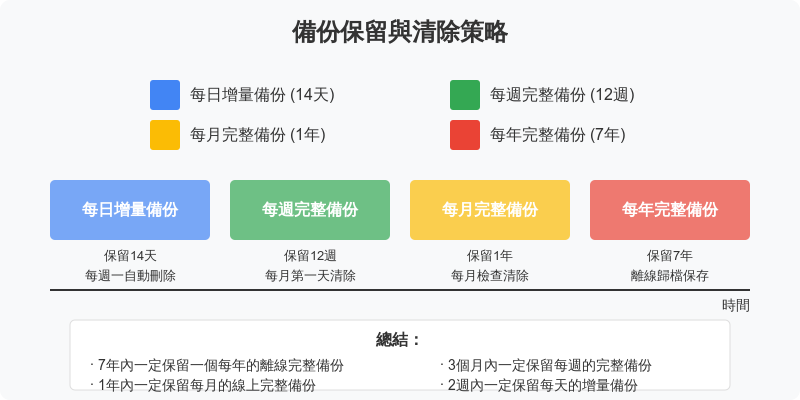


**備份機制**

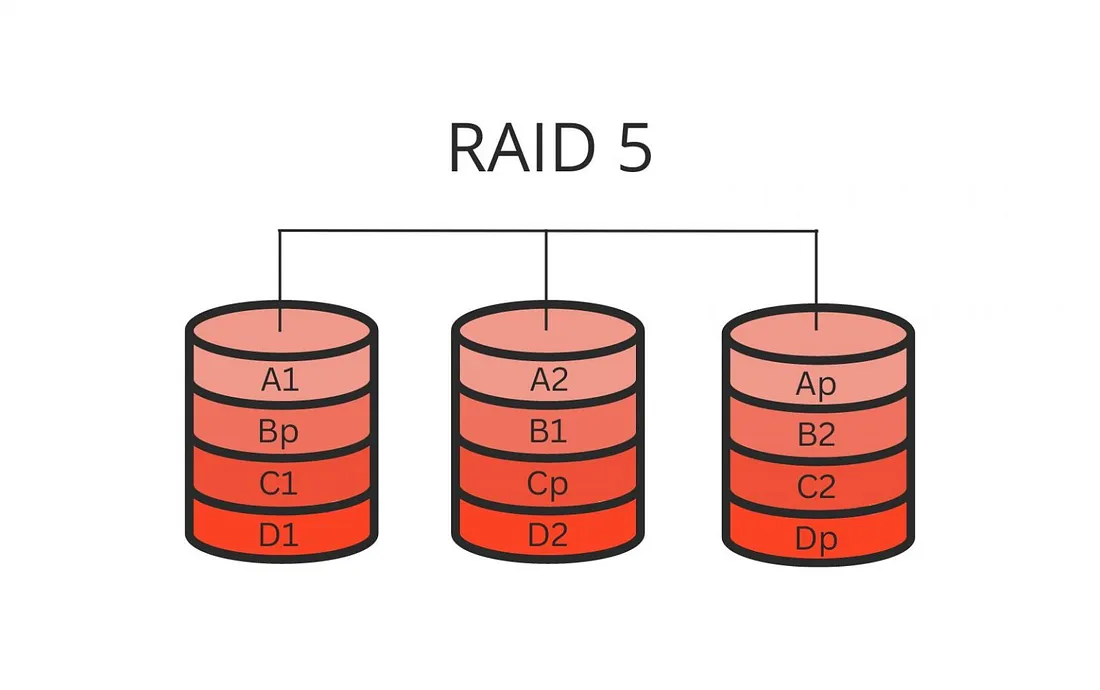
* 備份方式
* 完整備份 (Full Backup)：所有資料完整備份，不依賴其他備份檔案，資源需求高。
* 差異備份 (Differential Backup)：備份至最後一次完整備份以來的變更。
* 增量備份 (Incremental Backup)：備份至上次備份 (完整或增量) 以來的變更。
* 備份特性比較：
  + 備份時間：完整 > 差異 > 增量。
  + 備份容量：完整 > 差異 > 增量。
  + 還原時間：增量 > 差異 > 完整。
  + 還原所需檔案數量：增量 > 差異 > 完整。



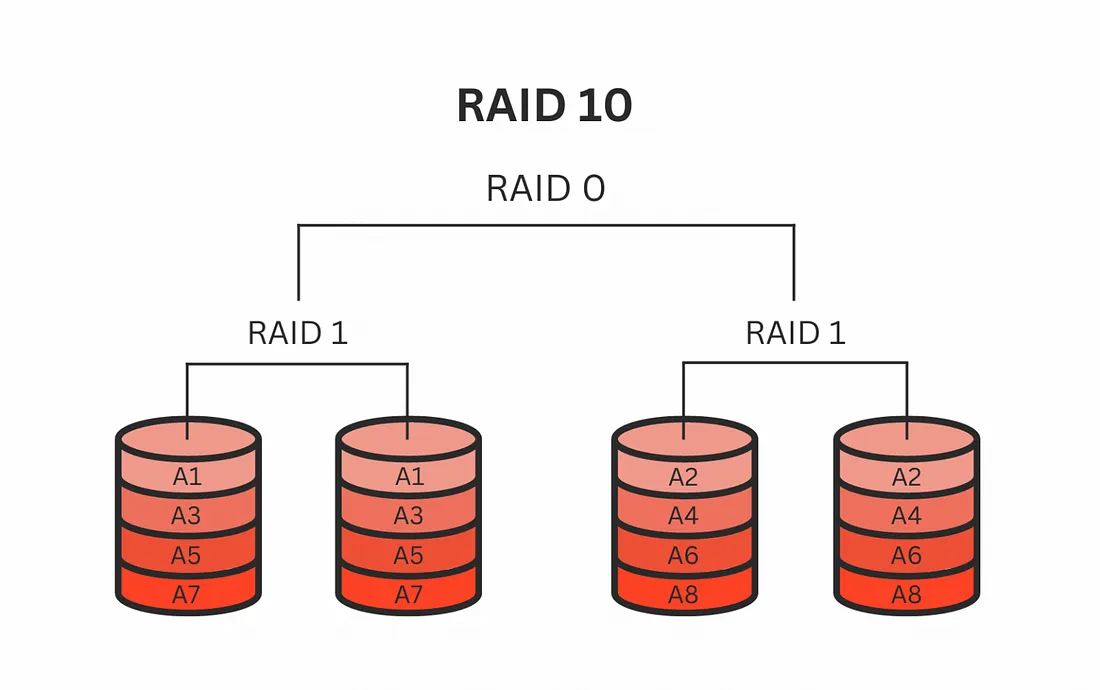
(資料來源：網際網路)



* RAID陣列
* RAID 0：無容錯，僅提升速度，最少 2 顆硬碟，容量為全部容量。
* RAID 1：鏡像資料，最少 2 顆硬碟，可壞 1 顆，容量為一半。
* RAID 5：加入容錯碼，最少 3 顆硬碟，可壞 1 顆，容量為 。
* RAID 6：加入容錯碼，最少 4 顆硬碟，可壞 2 顆，容量為 。
* RAID 10：結合 RAID 1 和 RAID 0，最少 4 顆硬碟，可壞 2 顆，但不能同時壞同一組，容量為一半。



(資料來源：網際網路)



(資料來源：網際網路)

* 備援場所
* 鏡像站點 (Mirror Site)
  + 也稱「同地（近地）/異地即時同步」或「Active-Active」架構
  + 與主要機房同步運行，資料即時更新，確保業務連續性
  + 成本及網路需求最高、恢復速度最快（可直接切換）
* 熱備援站點 (Hot Site)
  + 預先安裝系統、伺服器、網路設備，並定期或頻繁更新資料
  + 成本高、恢復速度快（可在數分鐘至數小時內接手）
* 溫備援站點 (Warm Site)
  + 已備妥必要硬體與網路設備，但需進一步設定或上載資料
  + 成本中等、恢復速度中等（可在數日或數星期內接手）
* 冷備援站點 (Cold Site)
  + 僅提供機房空間、電力、空調、網路基礎；無預先安裝任何系統或硬體
  + 成本最低、恢復速度最慢（可在數星期或數月內接手）
* 行動備援站點(Mobile Hot Site)：
  + 以卡車等可移動載具作為機房，內含基礎設備與系統
  + 可在災難時迅速移動至受災地點，作為臨時備援中心
* 互惠站點 (Reciprocal Site)
  + 多家機構（例如同類型組織，如醫院）簽訂互相支援協議
  + 當一方機房無法運作時，另一方可暫時提供其空間、設備或資源
  + 成本相對低，但依賴對方是否有足夠閒置資源，且需考量雙方的相容性與協調時間
* 特性比較：
  + 所需成本：鏡像 > 熱備援 > 溫備援 > 冷備援。
  + 恢復速度：鏡像 > 熱備援 > 溫備援 > 冷備援。
* 備份 3-2-1 原則
* 3份資料副本：本機一份、磁碟陣列一份、磁帶一份。
* 2種不同的媒介：磁碟陣列與磁帶。
* 1 份異地備份：磁帶存放於異地機房，遠離主要機房。

**營運持續演練**

* 檢查表測試 (Checklist Test)：
* 目的：主要透過檢查表方式，確保所有必要資源、人員聯絡資訊、程序文件都在位，沒有缺漏。
* 特點：成本與風險最低，但也最缺乏真實度。通常是第一步用來確認文件完整性。
* 結構化演練 (Structured Walkthrough)
* 目的：讓相關人員在會議室中，根據程序文件一步步討論並想像如何執行，找出未考慮到的情況。
* 特點：比檢查表測試更深入，可以透過集思廣益的方式讓各部門、人員同步了解流程，並及時發現缺失。
* 模擬測試 (Simulation Test)
* 目的：模擬實際情境，但不真正切換或停機；可能會在機房中進行「走流程」，或進行部分系統測試（例如測試備援系統啟動但不對外提供服務）。
* 特點：增加了現場操作的真實感，成本比前兩種高，卻能更有效地檢驗計畫的可行性。
* 並行測試 (Parallel Test)
* 目的：同時啟動備援系統與主要系統，觀察備援系統的運作狀態是否正常。
* 特點：若備援系統跑得順利，理論上可以無縫切換到備援系統；而主要系統持續運作，因此風險相對較小。但因為要同時維護兩邊系統，成本和人力需求相對提高。
* 完全中斷測試 (Full-Interruption Test)
* 目的：停止主系統，讓所有實際運作都移轉到備援系統進行；真正驗證「災難狀態下系統」的可用性。
* 特點：成本與風險最高，卻也是最真實、最能測出計畫缺陷的測試方式。若備援系統有問題，可能會直接影響正常營運，因此必須事先慎重規劃。
* 特性比較：
  + 越往下成本越高，但越真實。

**機房實體安全**

* 人員安全第一
  + 「第一鐵則：如果選項中有人員安全，一定是第一優先」是正確且重要的觀念。
* 災害防護：
* 水災：機房避開地下室與低樓層是一項常見建議，也可參考是否有防水閘門或排水設備。
* 火災：偵測系統（煙霧、溫度）與適合機房的滅火設備（如氣體滅火）是標配。
* 地震：異地備援機房確實通常建議在相隔三十公里以上，避免同個地區性災害的影響，可參考「我國電腦機房異地備援機制參考指引」。
* 空調系統
* 溫濕度：常見建議為 18-27°C、45-55% RH，也可依照 ASHRAE（美國暖通空調工程師協會）的標準做更精細的調整。
* 冷熱通道：規劃冷通道與熱通道以提高冷卻效率，也是現今機房的最佳實踐。
* 消防系統
* 滅火設備：
  + FM200 氣體為現行常見的氣體滅火系統，對電子設備影響較小。
  + INERGEN（惰性氣體）造價較高，但環境衝擊更低，適合對設備/環境要求更高的場所。
* 電力系統
* UPS：提供短暫備援電力及穩定電壓的功能：在市電斷電瞬間可立即接手供電，為關鍵設備爭取時間以執行正常關機程序或讓柴油發電機啟動，同時也負責電壓調節與濾波以保護設備。
* 柴油發電機：放置位置應同時考慮通風排氣、安全性、以及燃料補給便捷性（高樓層需要足夠電梯或運送管道）。
* 門禁故障模式
* Fail-Safe（失效安全）：斷電/故障時門自動解鎖，保護人員生命安全。
* Fail-Secure（失效安全防護）：斷電/故障時門保持上鎖，保護機房資產安全。
* 遇到火警時通常系統會自動切換到「安全模式」（即自動解鎖門），以確保人員能迅速撤離。

**考古題：**

10. 據NIST SP 800系列標準，關於災難復原計畫（Disaster Recovery Plan，DRP）、業務持續性計畫（Business Continuity Plan，BCP）和資訊系統應急準備計畫（Information System Contingency Plan，ISCP）的關聯性，下列何項描述正確？

(A) 災難復原計畫（DRP）專注於資訊技術系統的恢復，而業務持續性計畫（BCP）和資訊系統應急準備計畫（ISCP）則專注於組織的整體運營恢復

(B) 資訊系統應急準備計畫（ISCP）涵蓋整個組織的業務和資訊系統恢復策略，而災難復原計畫（DRP）和業務持續性計畫（BCP）則關注於特定技術解決方案

(C) 業務持續性計畫（BCP）專注於資訊技術系統的恢復，而災難復原計畫（DRP）和資訊系統應急準備計畫（ISCP）則專注於組織的整體運營恢復

(D) 災難復原計畫（DRP）專注於資訊技術系統的恢復，業務持續性計畫（BCP）涵蓋組織整體的業務運營持續性，而資訊系統應急準備計畫（ISCP）則專注於特定資訊系統的應急反應

防護 114-1 答案D

(根據NIST SP 800系列標準，

災難復原計畫（DRP）：專注於資訊技術系統在災難發生後的恢復。

業務持續性計畫（BCP）：涵蓋整個組織的業務運營持續性，確保在災難狀況下整體業務能持續運行。

資訊系統應急準備計畫（ISCP）：針對特定資訊系統的應急反應措施，確保在異常狀況下能快速反應與復原。)

20. 關於備份3-2-1原則的敘述，下列何者正確？

(A) 已儲存媒體而言，分開存放在兩種不同儲存媒體 (這是 3-2-1 原則中 "2" 的要求，目的是防止單一類型的儲存媒體故障（例如所有硬碟同時損壞）導致所有備份資料遺失)

(B) 至少三份，分別放到硬碟的C槽跟D槽 (違反 3-2-1原則的2，放在不同媒介裡)

(C) 資料分別存放在辦公室不同樓層 (一份放在異地)

(D) 備份資料不需備份加密金鑰

防護 113-2 答案A

23. H公司於上周發生公司 email超過 4個小時以上無法收發的資安事件，經 MIS人員處理後發現，郵件伺服器因硬碟空間不足而無法正常運作，並由追蹤相關記錄中找出服務中斷前，系統正在處理一封寄給全公司 2000位同仁的內部公告郵件，其之中被夾帶著 4GB的附檔，但此附檔在防毒軟體和沙箱工具檢查後並無病毒或威脅性，刪除此郵件及相關衍生作業後，郵件伺服器恢復正常運作，檢討此次內部資安攻擊事件， 確認為人員操作失誤所致。 請問下列哪些措施可以防範相關事件再度發生？（複選）

(A) 儘快增購郵件伺服器的硬碟容量，避免再發生相同空間不足的問題再度發生 (**有幫助，但非治本**。增加硬碟容量可以緩解問題，但無法從根本上解決問題。如果使用者繼續發送大檔案郵件，問題還是會再次發生。此外，過大的郵件不僅會影響郵件伺服器的效能，還會占用大量的網路頻寬)

(B) 對員工加強資安教育訓練，避免錯誤的資訊系統操作行為

(C) 增加防火牆檢查細則，減少大量或敏感資料的傳輸與攻擊事件 (**有幫助，但非主要針對此事件**。防火牆主要用於網路邊界的防禦，對於內部使用者發送大檔案郵件的行為，防火牆的作用有限。雖然可以設定規則來限制特定類型的檔案傳輸或限制傳輸大小，但主要還是要依靠郵件伺服器本身的設定和員工的安全意識。)

(D) 郵件伺服器增設郵件處理容量限制，阻絕大檔案的傳送服務

防護 113-2 答案BD

35. 請問下列何種備份策略，在還原時，只要當次備份的檔案及上一次完整備份檔案即可完成資料的還原？

(A) 完整備份配合增量備份

(B) 完整備份配合差異備份

(C) 複製

(D) 差異備份配合增量備份

技術 113-2 答案B

47. 關於組織進行營運衝擊分析所需包含之內容敘述，下列何者錯誤？

(A) 辨識關鍵業務相關之活動

(B) 辨識各活動中斷時，會對機關所造成的衝擊

(C) 確認各活動之最小可容忍中斷時間（Maximum Tolerable Period of Disruption, MTPD）

(D) 根據各活動復原之優先順序加以分類，藉以鑑別機關之關鍵活動

管理 113-2 答案C

(應該是「最大」可容忍中斷時間，而不是「最小」。MTPD 代表的是該活動可以中斷多久，而不會對組織造成不可接受的損害)

49. 災難發生時，下列何項是最重要的？

(A) 物理資產的保護

(B) 人員生命安全的保護

(C) 維持公司的股票價值

(D) 市場行銷活動的持續進行

管理 113-2 答案B

(人員生命安全的保護一定是最重要的)

50. 請問下列何項備援方式，異地備援機制所需時間最長？

(A) 冷備援（Cold site）

(B) 熱備援（Hot site）

(C) 溫備援（Warm site）

(D) 公司機房內建備援 (非異地)

管理 113-2 答案A

(冷>溫>熱)

32. 面對勒索軟體檔案加密的威脅，業界採用多重備份來事前預

防。關於業界常用的「3-2-1備份原則」的描述，下列何正確？

(A) 3是指三份備份、 2是指兩種不同儲存媒體、 1是指一份異地保存

(B) 3是指三個單位核准、 2是指兩個主管確認、 1是指一個人員備份

(C) 3是指三級單位執行、 2是指二級單位確認、 1是指一級單位稽核

(D) 3是指三種備份技術、 2是指二種備份流程、 1是指一個備份人員

技術 113-1 答案A

38. 某公司於每日的凌晨1點進行備分，每週日進行完整備份

（Full Backup），其餘各日進行增量備份（Incremental Backup），假設需要還原至週三下班時的狀況，需要下列何項備份檔案才能完成這樣工作？

(A) 該週日的備份即可

(B) 該週三的備份即可

(C) 該週日、一、二、三等4份的備份檔案

(D) 該週日、一、二、三、四等5份的備份檔案

技術 113-1 答案D

(週日提供完整備份作為基礎，週一、週二、週三的增量備份則依序包含了每一天新增或修改的資料)

46. 關於資訊備份的敘述，下列何者錯誤？

(A) 資訊允許可遺失的時間，就是備份必須實施的頻率依據

(B) 備份媒體因為有機密性的考量，所以適時的加密是要增加的機制

(C) 確認備份媒體的可用性，是定期需要實施的機制

(D) 備份媒體置放於異地後，無須定期盤點

管理 113-1 答案D

(異地備份媒體仍需定期盤點，以確保媒體安全存在且可正常使用，不能置之不理)

48. 試問有關復原時間目標（Recovery Time Objective RTO）與復原點目標（Recovery Point Objective RPO）之敘述，下列何者錯誤？

(A) 復原點目標是指在組織發生中斷事件後，該組織就業務面衡量其所保存資料與發生中斷前24小時之資料，差距有多少

(B) 復原點目標主要觀察與評判該機關執行資料備份與備份資料異地存放之頻率，以做為決定是否實施資料備份與備份頻率

(C) 復原時間目標是指機關於發生中斷事件後，該機關對於回復其所提供產品或服務之時間性目標

(D) 主要是做為機關衡量針對該關鍵活動所具備之營運持續能力

管理 113-1 答案A

(RPO是組織自行決定可接受的最大資料遺失時間，而非固定24小時)

49. 下列何種系統備援方案提供了最快的恢復時間？

(A) 熱備援

(B) 冷備援

(C) 暖備援

(D) 離線備份

113-1 答案A

(熱備援系統與主系統資料同步但須手動啟動切換，熱>暖>冷)

50. 異地備援為將企業內所需之資料/系統，分開兩地同步存放。請問關於異地備援的說明下列何項最「不」適切？

(A) 當一地發生事故時，另一地能持續接手運轉提供服務

(B) 有了異地備援便無資料丟失之風險

(C) 可適用於需要業務不中斷的企業組職

(D) 異地備援的建置可能導致投入成本增加

管理 113-1 答案B

(異地備援不能完全消除資料丟失風險，因為資料同步仍有時間差，且可能因網路中斷等因素影響同步)

19. 關於系統災害復原規劃的敘述，下列何項錯誤？

(A) 恢復點目標（RPO）的設定應考量資料備份頻率

(B) 最大可中斷時間（MTD）的設定，應符合組織所訂定之可用性的資安目標

(C) 恢復時間目標（RTO）之設定與最大可中斷時間（MTD）無關 (RTO要符合業務單位的最大可中斷時間，RTO < MTD)

(D) 營運衝擊分析（BIA）可協助評估各個系統的重要性

規劃 112-2 答案C

37. 當A公司的備份策略是每個月底最後一天的晚上6點後進行一次全備份，而每週六凌晨1點進行一次差異備份，假設所有備份檔案都完整，今天3月10日剛好是週五，中午時不幸系統中毒，所有資料遺失，請問當備份順利還原後，最近的資料是下列哪一天的備份？

(A) 2月28日

(B) 3月4日

(C) 3月9日

(D) 3月10日

技術112-2 答案B

(資料還原的步驟通常是：還原最近一次的全備份。依序還原全備份之後的差異備份，直到最接近資料遺失時間點的備份。在這個情境中：首先還原 2 月 28 日晚上6點的全備份。然後還原 3 月 4 日凌晨 1 點的差異備份)

38. 異地備援是資料備份最好的選擇，其復原速度最快的是下列何種方式？

(A) 冷備援（Cold Site）

(B) 暖備援（Warm Site）

(C) 熱備援（Hot Site）

(D) 全備援（Mirrored Site）

技術112-2 答案D

(復原速度：鏡>熱>暖>冷，全備援就是鏡備援)

46. 關於備份的敘述，下列何者較正確？

(A) 因為資源的分配，所有需要備份的資料都是每天備份一次 (按照重要性)

(B) 備份的頻率應該依照所需備份資料的重要性來分配

(C) 備份於磁帶的資料可儲存於同層樓的辦公室 (違反備份3-2-1原則的1，異地一份)

(D) 備份可儲存於同一台硬體設備上 (違反備份3-2-1原則的2，不可放在同一個媒介)

管理 112-2 答案B

(不同重要程度的資料需要不同的備份頻率，重要資料需更頻繁備份以降低資料遺失風險，並且按照備份3-2-1原則，需要在異地留一份資料。)

47. 關於營運持續規劃階段的敘述，下列何者較正確？

(A) 組織在規劃營運持續時，須將所有的資訊系統納入 (不是「所有」系統都要納入，應該依據營運衝擊分析(BIA)的結果，優先納入重要系統和關鍵業務)

(B) 組織應以目前資訊系統資源，來規劃資訊系統營運持續的實施 (不應受限於「目前」的資源，應該根據組織需求來規劃所需資源，可能需要投入新的資源來確保持續營運)

(C) 組織於營運持續規劃的階段就須將資訊安全納入考量

(D) 營運持續的規劃因為資源的限制，以同地做為考量即可 (不能「只」考慮同地備援，應該考慮異地備援的可能性，災難可能影響整個地理區域)

管理 112-2 答案C

48. 關於資訊處理設施備援規劃的敘述，下列何者錯誤？

(A) 組織可視資訊系統允許中斷時間要求，備妥資訊處理設施所需數量，以符合可用性之目標 (RTO < MTPD)

(B) 考量資訊處理設施備援規劃時，不只主機相關設備的備援，亦需要考慮到其他支援設施，如：發電機等 (油、水和電都要考慮)

(C) 規劃資訊處理設施的備援時，以可用性要求為主，不需要特別考慮機密性或完整性的議題 (機密性、完整性和可用性都要考慮)

(D) 規劃維持營運持續使用到的備援設備，也需要安排時間確認其可用性 (備援計劃都要經過演練才能了解是否可用性)

管理 112-2 答案C

49. A公司災害緊急應變措施對於重要系統資料的恢復點目標（

Recovery Point Objective, RPO）設定為 4小時。關於此公司重要系統資料的備份週期，下列何項最適合？

(A) 每 2小時備份

(B) 每日備份

(C) 每 8小時備份

(D) 每週備份

管理 112-2 答案A

(RPO為4小時代表最多容許遺失4小時的資料，所以備份頻率要在4小時內，選2小時備份才能確保達標。)

50. 在組織遇到資安事件時，可能需要尋找適宜的替代場地，請問關於替代場地的敘述，下列何者較正確？

(A) 冷備援站點（Cold site）：場地和設備皆有，於事件發生時依需求執行回復工作(暖備援站點)

(B) 暖備援站點（Warm site）：異地備援端備有同樣之系統，事件發生時在可接受的時間內恢復啟用，待資料載入後即可投入營運 (熱備援站點)

(C) 熱備援站點（Hot site）：有提供基本設備，但仍須自行安裝系統(冷備援站點)

(D) 行動備援站點（Mobile hot site）：在移動車輛中安裝設備與系統，當事件發生時，可迅速移動至適當地點啟用

管理 112-2 答案D

(行動備援站點是在移動車輛中預先安裝好設備與系統，需要時能快速移動到指定地點啟用作為臨時營運場所。)

23. 關於備份 3-2-1原則的敘述，下列何者正確？

(A) 以儲存媒體而言， 分開存放在兩種不同儲存媒體

(B) 至少三份，分別放到硬碟的Ｃ槽跟Ｄ槽 (這通常意味著在同一物理設備上的不同分區。這不符合 3-2-1 原則中的第三點，即至少有一份備份應存放在異地。)

(C) 資料分別存放在辦公室不同樓層 (將備份存放在不同樓層確實增加了物理上的隔離，但這並不等同於「異地」存放。3-2-1 原則中的「異地」通常指不同的地理位置，以防止整個辦公場所遭受災害。)

(D) 備份資料不需備份加密金鑰 (如果備份資料是加密的，則備份加密金鑰是至關重要的。沒有加密金鑰，備份資料將無法解密和使用。因此，備份加密金鑰是確保資料可用性的必要步驟。)

防護 112-1 答案A

36. 關於電腦檔案備份的敘述，下列何者錯誤？

(A) 檔案備份首重擬定備份策略，以確實發揮資料還原效果

(B) 將資料依重要性程度加以區分，在訂定資料備份策略時，才能掌握真正需要備份的標的

(C) 完整備份：備份空間有限的狀況下，十分適合使用完整備份

(D) 備份位置主要可分為「本機備份」、「異機備份」及「異地備份」三種不同方式

技術 112-1 答案C

(如果考慮到備份空間有限的狀況下，應使用增量備份，這種方式使用空間最少，備份容量：完整 > 差異 > 增量)

37. 請問下列何種備份策略，所需的儲存空間最少？

(A) 全備份配合增量備份 (使用空間最少)

(B) 全備份配合差異備份 (使用空間次之)

(C) 複製 (因為每次都全備份，使用空間最多)

(D) 差異備份配合增量備份 (差異備份和增量備份都需要依賴完整備份)

技術 112-1 答案A

38. 在「行政院及所屬機關資訊安全管理規範」的日常作業之安全管理中，下列關於「資料備份」的作業原則何者錯誤？

(A) 資料應另外存放在離機關近距離的作業場所，以利方便存取

(B) 重要資料的備份，以維持三代為原則

(C) 備份資料應有適當的實體及環境保護，應以原主要作業場所為標準

(D) 資料的保存時間需求，應由資料擁有者研提

技術 112-1 答案A

(參考「我國電腦機房異地備援機制參考指引」中，異地備份/備援機制提及之主機房與異地備援機房之距離應距離30公里以上，宜朝「不遭受同一風險或事件影響」的方向考量)

42. 下列何者較「不」是持續營運資料備份的考量項目？

(A) 場地大小

(B) 存放位置

(C) 成本高低

(D) 安全性

管理 112-1 答案A

(存放位置例如要距離30公里才不會相同的風險，成本和安全性也是很重要)

43. 關於營運衝擊分析及災害復原計畫應考慮項目，下列敘述何者最「不」正確？

(A) 復原至最小營運水準所需之員工、技術、設施及服務所需之時間

(B) 損害程度之等級不包括收入損失、附加成本、商譽損失、喪失競爭優勢等

(C) 最小營運水準所需之人員、系統軟體及硬體及交通等，皆為須考量之資源

(D) 復原時間是完全復原至原服務水準所需之員工、技術、設施及服務所需之時間

管理 112-1 答案B

(損害程度包含有形資產和無形資產，有形包含金錢上的損失，無形包含公司商譽)

47. 營運衝擊分析最主要的目的為何？

(A) 進行風險分析

(B) 確認重要流程的最大可承受中斷時間

(C) 記錄結果，並提出改正措施

(D) 確認殘餘風險

管理 112-1 答案B

(營運衝擊分析主要是確認企業各業務流程能容忍的最大中斷時間，以制定適當的營運持續計畫)

48.關於資料備份的敘述，下列何者正確？

(A) 因為資源設備的限制，無須進行回復測試 (回復測試很重要，才知到備份有無成功)

(B) 備份儲存媒體上的資料可永久保存 (應指定保存政策)

(C) 備份媒體儲存的地點，需考量主要地點發生災難時，不會被波及的場域

(D) 因為備份工具每天皆會啟動進行備份，所以若當日無法備份完成，隔日成功即可 (備份失敗要立刻找尋原因並重新執行備份)

管理 112-1 答案C

49. 若是A公司不能接受重要系統中斷超過1小時，下列何項異地備援方式最適合該公司？

(A) 冷備援

(B) 熱備援

(C) 溫備援

(D) 機房內自主備援

管理 112-1 答案B

(只能接受1小時內系統中斷的情況必須採用熱備援，因為熱備援系統資料趨近於即時同步，可以最快速地切換恢復服務。)

50. X公司對於電子郵件系統可用性目標設定為不得中斷超過一天，在制定該系統災害復原計畫時，關於此公司復原時間目標（Recovery Time Objective, RTO）的設定，下列何項最適當？

(A) RTO設定為二天

(B) RTO設定為一週

(C) RTO設定為20小時

(D) 在制定災害復原計畫時，不需考慮RTO

管理 112-1 答案C

(系統不能中斷超過一天（24小時），所以RTO要設定在一天以內的20小時才能確保達到可用性目標，設定更長時間會違反需求。)

50. 下列何者「不」是營運持續性的相關用語？

(A) 交叉錯誤率（Crossover Error Rate, CER）

(B) 營運衝擊分析（Business Impact Analysis, BIA）

(C) 復原時間目標（Recovery Time Objective, RTO）

(D) 最大可容忍中斷時間（Maximum Tolerable Downtime, MTD）

管理 112-1 答案A

(A選項CER是存取控制相關用語)

35. 若公司營運系統伺服器內有三顆硬碟作 RAID 5，並且備份機制中規劃每週五 23:00進行完整備份（Full Backup），其餘每天 23:00進行增量備份（Incremental Backup）已持續運行半年狀況很好，無奈於本週一11:00時伺服器其中一顆硬碟發生故障，請問應採取下列何種處理方式？

(A) 將上週五的Full Backup磁帶回存，再將六、日的增量備份磁帶回存

(B) 將上週五的Full Backup磁帶回存，再將週日的備份磁帶回存

(C) 更換有問題的硬碟即可

(D) 更換有問題的硬碟，並將上週五的Full Backup磁帶回存，再將六、日的增量備份磁帶回存

技術 111-2 答案C

(C選項更換有問題的硬碟即可。此操作可透過RAID 5的冗餘機制自動重建數據，確保系統恢復正常運作)

37. 請問利用磁帶進行資料備份時，執行備份時耗時較久，但回復時需要的磁帶數通常最少的是下列何者？

(A) 巨量備份（Bigdata Backup）

(B) 完全備份（Full Backup）

(C) 差異備份（Differential Backup）

(D) 增量備份（Incremental Backup）

技術 111-2 答案B

(完全備份的特性為執行備份時耗時較久但需要的磁帶數通常最少)

2. 「 M公司的資訊系統，每週均有進行系統與資料備份，且有異地備

份，而近期公司增加了新多重加密機制，讓資料安全可以進一步確

保。然近期進行系統之復原測試時，發現復原作業時間共需要 6小

時，與公司的規定4小時，明顯不符。」關於上述案例中，「不」符

合下列何者要求？

(A) 復原時間目標（Recovery Time Objective, RTO）

(B) 復原點目標（Recovery Point Objective, RPO） (指在系統故障後，允許的最大資料丟失量，通常以時間來衡量。此案例中並未提及數據丟失的情況)

(C) 平均復原時間（Mean Time to Recovery, MTTR）(指平均每次復原所需的時間。雖然實際復原時間較長，但問題的焦點在於是否符合公司規定的目標，而非平均值)

(D) 平均失效時間（Mean Time to Failure, MTTF）(指系統平均運行多長時間會出現一次故障。此案例中沒有涉及系統故障的頻率)

規劃 111-1 答案A

(指在系統故障後，允許的最大復原時間。案例中實際復原時間6小時超過了公司規定的4小時，不符合RTO)

11. 磁碟陣列（RAID）是指使用多個磁碟進行資料複製的檔案系統，它是一種即時備援與資料復原技術，若以硬碟毀損方面進行評估，下列何種規劃對於資料保存的安全性最低？

(A) AD主機採用 2顆 SATA硬碟規劃成 RAID1 (1顆硬碟故障)

(B) 網路儲存裝置（NAS）採用 8顆 SATA硬碟規劃成 RAID5 (1顆硬碟故障)

(C) 檔案伺服器採用 4顆 SAS硬碟規劃成 RAID0 (RAID0沒有資料保護)

(D) 儲存區域網路（SAN）採用 16顆 SAS硬碟規劃成 RAID6 (2顆硬碟故障)

防護 111-1 答案C

13. 下列敘述何者較「不」正確？

(A) RTO 時間越長，代表可容忍系統無法使用時間越長

(B) RPO 的時間點要求越遠，代表可允許之資料備份週期越長

(C) RPO 的時間點要求越遠，代表可允許之資料備份週期越短

(D) MTPD 時間越長，代表可容忍系統無法使用時間越長

管理 111-1 答案C

(RPO的時間點要求越遠，表示可容忍遺失資料較多，代表可允許之備份週期越長)

14. 常見的磁碟陣列（Redundant Array of Independent Disks, RAID）中，RAID5 可以容忍同時幾顆硬碟損毀？

(A) 1

(B) 2

(C) 3

(D) 4

管理 111-1 答案A

48. 關於差異備份，下列敘述何者較為正確？

(A) 只備儲存媒體內自上次完全備份後曾更改或新增的檔案

(B) 只備儲存媒體內自上次備份後曾更改或新增的檔案

(C) 只備儲存媒體內第三次備份後曾更改或新增的檔案

(D) 只備儲存媒體內自上次完全備份後曾新增的檔案

管理 111-1 答案A

49. 下列何者「不」屬於營運持續計畫之演練方式？

(A) 模擬測試

(B) 檢查表測試

(C) 黑箱測試

(D) 完全中斷測試

管理 111-1 答案C

(營運持續計畫之演練方式包含

檢查表測試

結構化演練

模擬測試

並行測試

完全中斷測試)

15. 在其他備份環境與條件相同情況下，下列何者備份方式，其還原時速度最慢？

(A) 完整備份（Full Backup）

(B) 差異備份（Different Backup）

(C) 增量備份（Incremental Backup）

(D) 選擇式備份（Selective Backup）

技術 111-1 答案C

(增量>差異>完整)