新北市政府教育局
校園資安事件應變處理作為

講師：葉益禎

中華民國111年11月22日

課程大綱

序號	大綱
一	資安事件類型及通報應變相關規定
二	行政院頒布各機關資通安全事件通報及應變處理作業程序介紹
三	資安事件緊急應變處理方式
四	營運持續基本觀念與實作
五	問題與討論

資安事件類型及通報應變相關規定

資通安全事件定義

資通安全事件：

依『資通安全管理法』定義，指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響系統機能運作，構成資通安全政策之威脅。

- 從設備故障、人員差錯、人為事件或自然事件之類的單一事件到各種事件的複雜組合均屬於資安事件範疇內的事件案例

資通安全事件通報及應變辦法

資通安全事件的類型

- 內部事件
  - 遭人為惡意破壞毀損、作業不慎等危安事件
  - 設備故障
    - 能直接或間接影響機房安全資訊系統的各個設備的故障可視爲資安事件
  - 人員差錯
    - 錯誤的或不良的維護、錯誤設定和操作員的其他錯誤行為
  - 其他內部事件
    - 內部原因引起的火災、爆炸等對機房安全也可能產生重要影響

5

資通安全事件的類型(續)

- 外部事件
  - 自然事件或外部事件引起某一安全重要系統、元件和建築物故障的可能性，通過設計和建造中所採取的措施可降低到可接受的程度
    - 病毒感染事件
    - 駭客攻擊（或非法入侵）事件
  - 自然事件
    - 天然災害：颱風、水災、地震
    - 重大突發事件：停電、火災、爆炸、核子事故

6

駭客利用合法DLL之木馬程式攻擊

針對亞洲國家之新一波網路攻擊

美國資安廠商賽門鐵克9月13日發布文章，說明先前利用ShadowPad遠端存取木馬程式(Remote Access Trojan, RAT)攻擊手法之駭客組織，近期採用新攻擊手法攻擊亞洲政府與國營企業，目標包括政府部門與國營之金融機構、航太與國防、電信公司、IT組織及傳播媒體等，這些攻擊自2021年初開始，主要目的為情報蒐集。

攻擊特徵

該駭客組織使用DLL側載入(DLL Side-loading)手法，利用合法程式載入惡意dll檔案並執行攻擊。近期攻擊活動中駭客使用Infostealer.Logdatter替代原ShadowPad工具，以竊取鍵盤紀錄、螢幕截圖、連接與查詢資料庫、下載檔案及剪貼簿資料等。

猜測

賽門鐵克認為該攻擊手法與中國官方支持之APT41與Mustang Panda駭客組織曾使用之技術相似，中國駭客可能為這些攻擊活動之幕後黑手。

資料來源：09/14/2022技術服務中心

北韓各種社交工程手法攻擊南韓官員

北韓駭客組織Kimusky針對南韓政府官員進行網路攻擊

自2022年以來，北韓駭客組織Kimusky持續針對南韓之政治與外交單位進行攻擊。Kimsuky為北韓進階持續威脅(Advanced Persistent Threat, APT)組織，主要針對南韓進行網路攻擊，以獲取政治相關情報。該組織自2012年開始活動，曾採用**社交工程攻擊、魚叉式釣魚郵件攻擊及水坑攻擊(Watering hole attack)**，目的為竊取受駭者機敏資訊。

- ☑ 近期攻擊手法為**魚叉式釣魚郵件**，郵件中包括**檔案下載連結**，下載之檔案為嵌入惡意巨集之Word文件，此文件包括南韓政治地緣相關內容。
- ☑ 此攻擊不同於以往，受駭者點選電子郵件內之連結，會將電子郵件地址傳送至第1個中繼站並確認是否為正確之地址，若相同即將IP傳送至第2個中繼站。
- ☑ 當受駭者打開檔案後會將IP傳送至第2個中繼站，並驗證是否與第1個中繼站傳送之IP相符合，如相同才會下載Visual Basic腳本至受駭者電腦並進行後續攻擊，最終回傳檔案列表、鍵盤紀錄及瀏覽器登入憑證等資訊給駭客。
- ☑ 確認開啟電子郵件之IP與開啟檔案之IP是否一致之行為，顯示該攻擊手法具有**高度針對性**。

資料來源：08/31/2022 技術服務中心

俄國駭客組織持續攻擊烏克蘭

俄羅斯駭客組織Gamaredon持續攻擊烏克蘭

Gamaredon為俄羅斯政府支援之駭客組織，自2014年以來持續以烏克蘭為目標發動數千次攻擊。2022年2月俄羅斯入侵烏克蘭後，該駭客組織將攻擊重心著重於釣魚攻擊與散佈惡意程式。

勒索軟體攻擊 - 1	主要為帶有7-Zip壓縮檔附件之釣魚郵件攻擊，該檔案於解壓縮後執行資料竊取程式，駭客為躲避檢測亦修改不同版本。
勒索軟體攻擊 - 2	駭客使用VBS下載器下載Pterodo後門程式，此後門為Gamaredon自行開發之惡意程式之一，允許駭客錄製音訊、螢幕截圖、記錄鍵盤敲擊紀錄或下載其他程式並執行。近期駭客甚至利用合法遠端桌面程式控制受駭者電腦，如Ammyy Admin與AnyDesk。
攻擊活動 - 1	為利用PowerShell執行惡意程式並竊取瀏覽器之資料。
攻擊活動 - 2	駭客試圖利用自製巨集修改受駭電腦上之Normal.dotm檔案，此檔案為Microsoft Word範本，修改後將導致之後新建之Word檔案皆含有病毒，若使用者以電子郵件寄送Word檔案，將造成嚴重後果。

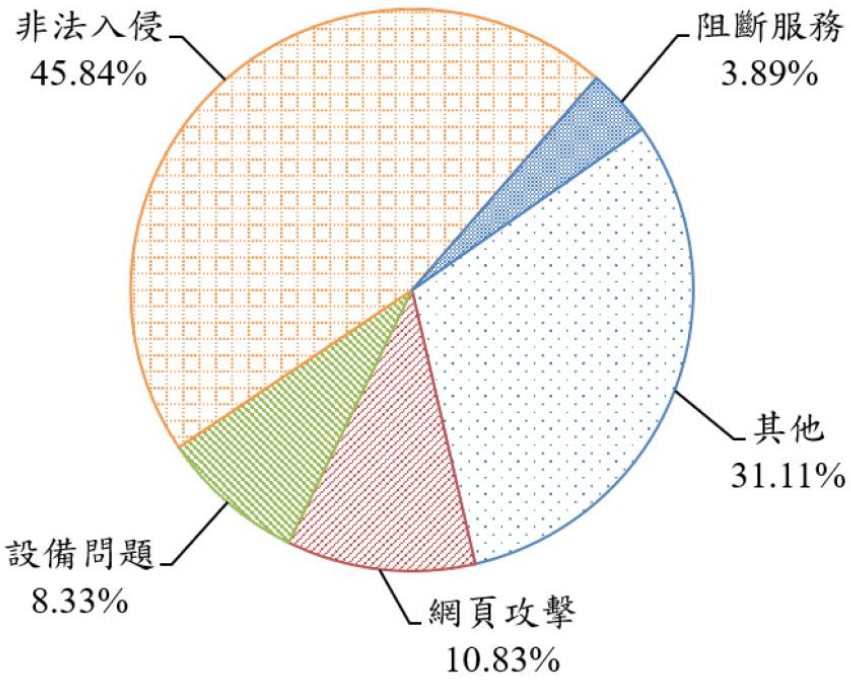
資料來源：08/15/2022技術服務中心

最新全球資安議題

- **社群媒體遭駭或利用，成為駭客謀利工具**
  - 現在駭客將目標擴大至社群媒體，英國陸軍推特帳戶及YouTube頻道分別擁有逾36萬名粉絲與18萬人訂閱，近期同時遭駭客入侵，其推特頁面遭，並於推文中假借NFT行銷活動之名，夾帶惡意連結。
  - 駭客利用YouTube假借遊戲教學或破解攻略影片，卻於影片中夾帶惡意軟體套件組，因為在此惡意軟體套件組中，有一合法之Nirsoft、NirCmd公用程式，可以在不啓動任何視窗下執行動作，因此更讓使用者難以發現其蹤跡。
- **採用新式間歇性加密(Intermittent Encryption)技術已成為勒索軟體之最新趨勢**
  - 只加密目標文件之部分檔案內容，以加速受駭者系統之加密速度。因其只加密部分內容，所以加密過程幾乎只需完全加密一半時間，且若不使用有效之解密方法與密鑰，仍無法使資料回復，依據此加密方式，將使過往偵測工具慣用檢測方式，無法有效且即時偵測異常狀況。
  - LockFile為第一個使用間歇性加密之勒索軟體，依每16位元組之間隔執行加密。
- 資料來源：技服中心 111年第3季資通安全技術報告

發現電腦遭綁架時簡要緊急應變措施

111年第3季政府機關通報資安事件類型

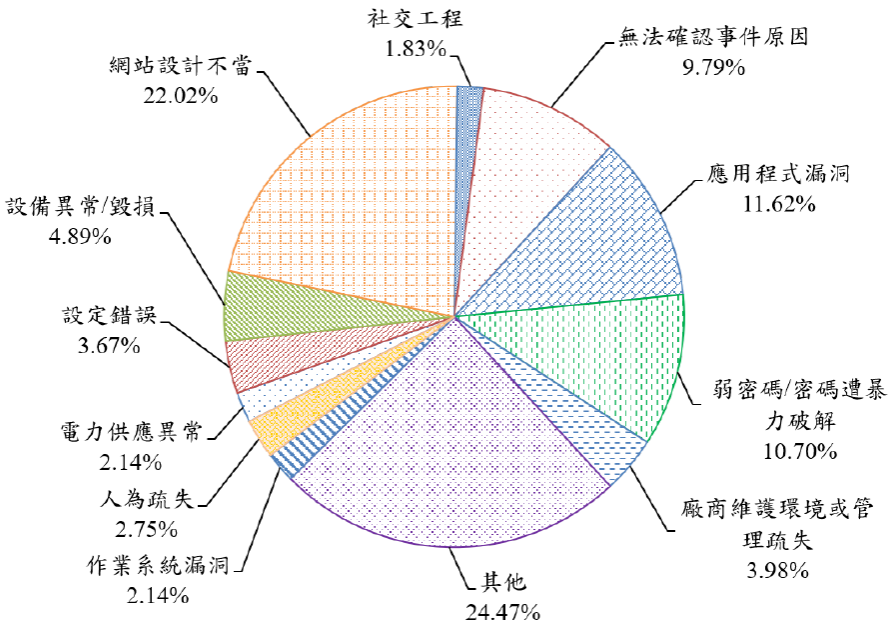


■ **重大事件**

- 發生個人電腦遭勒索軟體加密事件
- 部分機關電子看板或網站顯示之資訊遭惡意置換

資料來源：技服中心 111年第3季資通安全技術報告

111年第3季政府機關通報資安事件發生原因



■ 事件發生原因

- 使用者瀏覽網站時，點擊下載偽冒成微軟更新檔之程式
- 系統雖使用SSH(Secure Shell)加密連線登入，惟管理帳號使用弱密碼致遭暴力破解
- 弱密碼部分發現仍有機關以常見鍵盤位置排序(如1qaz@WSX)設置郵件密碼，雖符合密碼設定安全性原則，惟已列入駭客常見之暴力破解清單

資料來源：技服中心 111年第3季資通安全技術報告

資安與個資案例介紹-1

- 勒索病毒肆虐，雲林縣教育處縣網中心也中毒！11月4日許多國中小家長發現學校網頁無法進入，紛紛打電話向學校查問，才知道是縣網中心中毒，勒索病毒鎖住學校網頁，無法查看公告、學生成績，大家擔心孩子成績遭篡改，紛紛要求縣府盡速修復
- 雲林縣政府教育處縣網中心公告全縣186所國中小網頁被綁架無法開啟，不僅家長無法上網查詢公告，學校與師生的資料都被鎖死，13日縣府教育處表示已救回8、9成資料，目前各校網頁由網管人員重新建構，預計15日可恢復正常

資料來源：中時新聞網 110年11月14日

資安與個資案例介紹-2

- 台南市調查處接獲檢舉，在今年指考完後，補習班開始招生之際，有民眾持人頭電話四處兜售全國學生個資，專案小組在今年9月間發動第一波搜索，查獲負責販售個資陳男，循線追查至其上游，知名補習班蔡姓數學老師，調查後發現，蔡男涉嫌自2015年起，與駭客柴男及張男合作進行上述不法行為
- 該批750萬餘筆學生個資，內容包含學校名稱、年級、班級、姓名、身分證統一編號、父母姓名、父母職業、住址、聯絡電話及會考成績等資料，幾乎全國家中有就學子女者個資均被盜取，並以每筆個資新台幣10元至20元價格轉售予補習班業者

資料來源：ETToday新聞雲2021年11月17日

個資法解析

- 意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

資安與個資案例介紹-3

史上頭一遭！大考中心被駭客入侵 2千筆考生資料遭駭

- 教育部表示，大考中心在110學年試辦考試的報名系統，查獲有不明人士透過不當手段，進入試辦考試報名系統，觸及當時存於資料庫中部分學生的報名資料，大考中心即依法通報權責主管機關，實施緊急應變措施，並進行系統調整及強化資通安全防護措施，同時委請第三方公正單位進行事件調查與鑑識
- 目前清查，疑似有少部分學生報名資料經不明人士瀏覽（約 2,000 筆，占當時總數的 2.76%），大考中心已依個人資料保護法第12條及個人資料保護法施行細則第 22 條規定通知相關當事人；大考中心強調，這次事件與110指考報名系統並無關聯
- 大考中心對此表達遺憾與歉意，除已修正系統邏輯判斷缺失外，並已強化集報單位密碼強度，以避免類此事件再次發生。目前全案送司法調查中，同時也依資通安全事件通報及應變辦法進行通報與損害復原作業

資料來源：2021/06/01 Newtalk

資安與個資案例介紹-4

- 台灣大學前學生會長吳奕柔在臉書發文指出，昨天晚上登入台大師資培育中心的教育學程網路報名系統，發現只要輸入任何台大在學學生的學號，就可帶出學生的姓名、身分證字號、生日、手機電話、戶籍地址等個人資料
- 教務處昨天接獲通報後，已立即撤下該報名網頁系統，進行修復補強後重新上線，原本該教育學程招生考試報名時間為6月2日截止，因系統緊急維修，報名時間也延長至6月3日。台大校方指出，會檢討相關疏漏之處，未來也會強化相關資安要求與個資保護，並積極改善

資料來源：110/6/3 聯合報

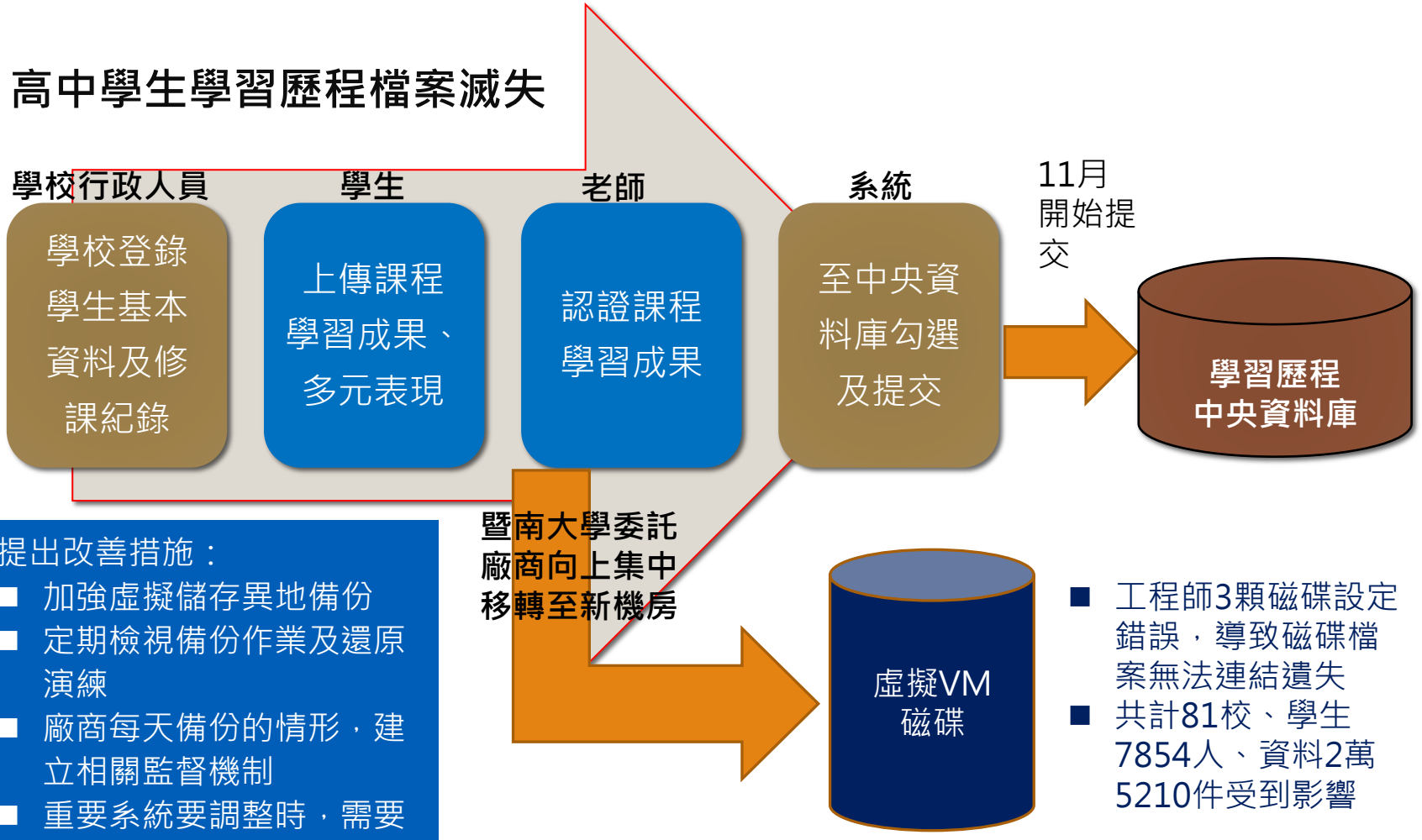
資安與個資案例介紹-5

- 國立臺南女中疑似個資外洩，學校利用線上表單服務蒐集新生資料，惟表單設定錯誤致使用者填完表單後可查看他人資訊
- 110學年度新生基本資料，欄位包含班級、姓名、性別、身分證字號、生日、地址、電話、個人及家庭概況等資料。疑似洩漏個人資料約613筆
- 學校進行資安通報，並於網站公告通知當事人

資料來源：110/9/1國立臺南女中網站

資安與個資案例介紹-6

■ 高中學生學習歷程檔案滅失



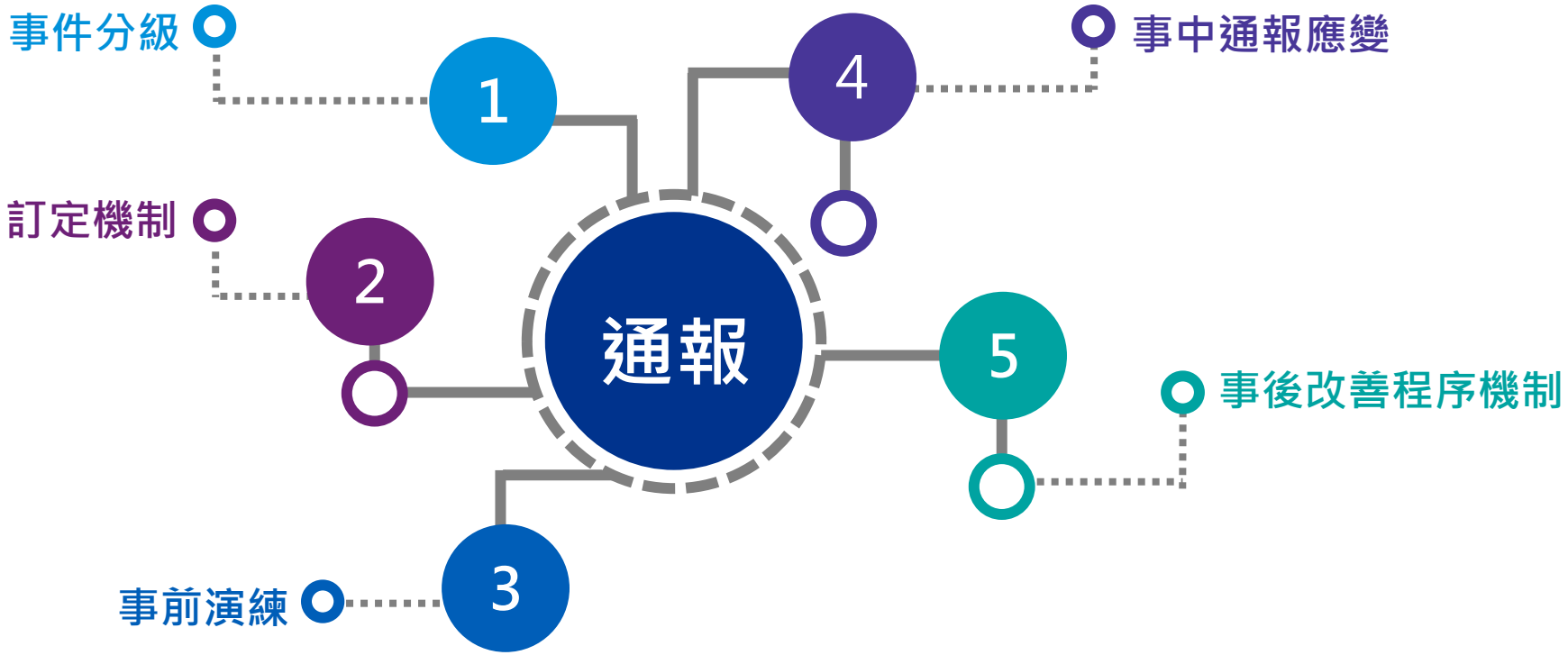
提出改善措施：

- 加強虛擬儲存異地備份
- 定期檢視備份作業及還原演練
- 廠商每天備份的情形，建立相關監督機制
- 重要系統要調整時，需要有專家全程在場監督或提供建議

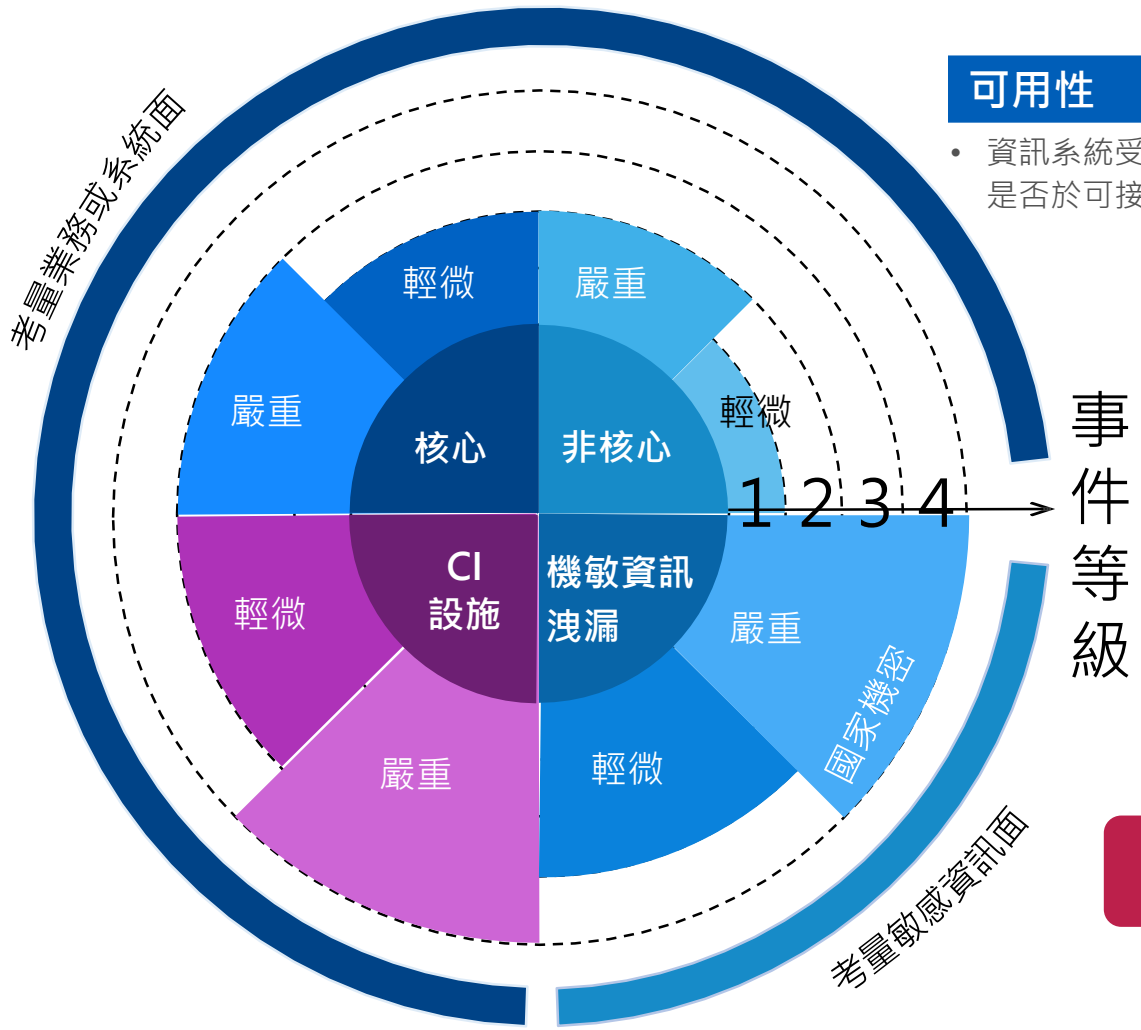
- 工程師3顆磁碟設定錯誤，導致磁碟檔案無法連結遺失
- 共計81校、學生7854人、資料2萬5210件受到影響

資通安全事件通報及應變辦法

- 為強化各機關之資安事件之因應
- 規範事件之分級、事前演練、事中通報及應變，以及事後改善之程序、機制



資通安全事件分級



機密性

- 業務資訊遭洩漏

可用性

- 資訊系統受影響或停頓，是否於可接受時間內回復

事件輕微或嚴重-考慮C,I,A三面向

完整性

- 業務資訊遭竄改
- 資通系統遭竄改

同一資安事件影響二個以上機關，等級向上提升一級

資通安全事件分級

判斷因素			第一級	第二級			第三級				第四級	
資訊洩漏(機密性)			非核心業務	• 核心業務 • 關鍵基礎設施非核心業務			• 一般公務機密 • 敏感資訊 • 關鍵基礎設施核心業務				國家機密	
資訊/資訊系統遭竄改狀況(完整性)	資訊竄改	資訊別	非核心業務	非核心業務	核心業務	關鍵基礎設施非核心業務(A)	核心業務	• 一般公務機密 • 敏感資訊	關鍵基礎設施非核心業務(A)	關鍵基礎設施非核心業務(B)	關鍵基礎設施非核心業務(B)	國家機密
		嚴重程度	輕微	嚴重	輕微	輕微	嚴重	--	嚴重	輕微	嚴重	--
	系統竄改	資通系統別	非核心	非核心	核心	處理(A)	核心	核心	處理(A)	處理(B)	處理(B)	處理(B)
		嚴重程度	輕微	嚴重	輕微	輕微	嚴重	嚴重	嚴重	輕微	嚴重	嚴重
受影響於容忍時間回復與否(可用性)	業務/資通系統別		非核心	非核心	核心	(A)	核心	核心	(A)	(B)	(B)	(B)
	可否回復		可	否	可	可	否	否	否	可	否	否

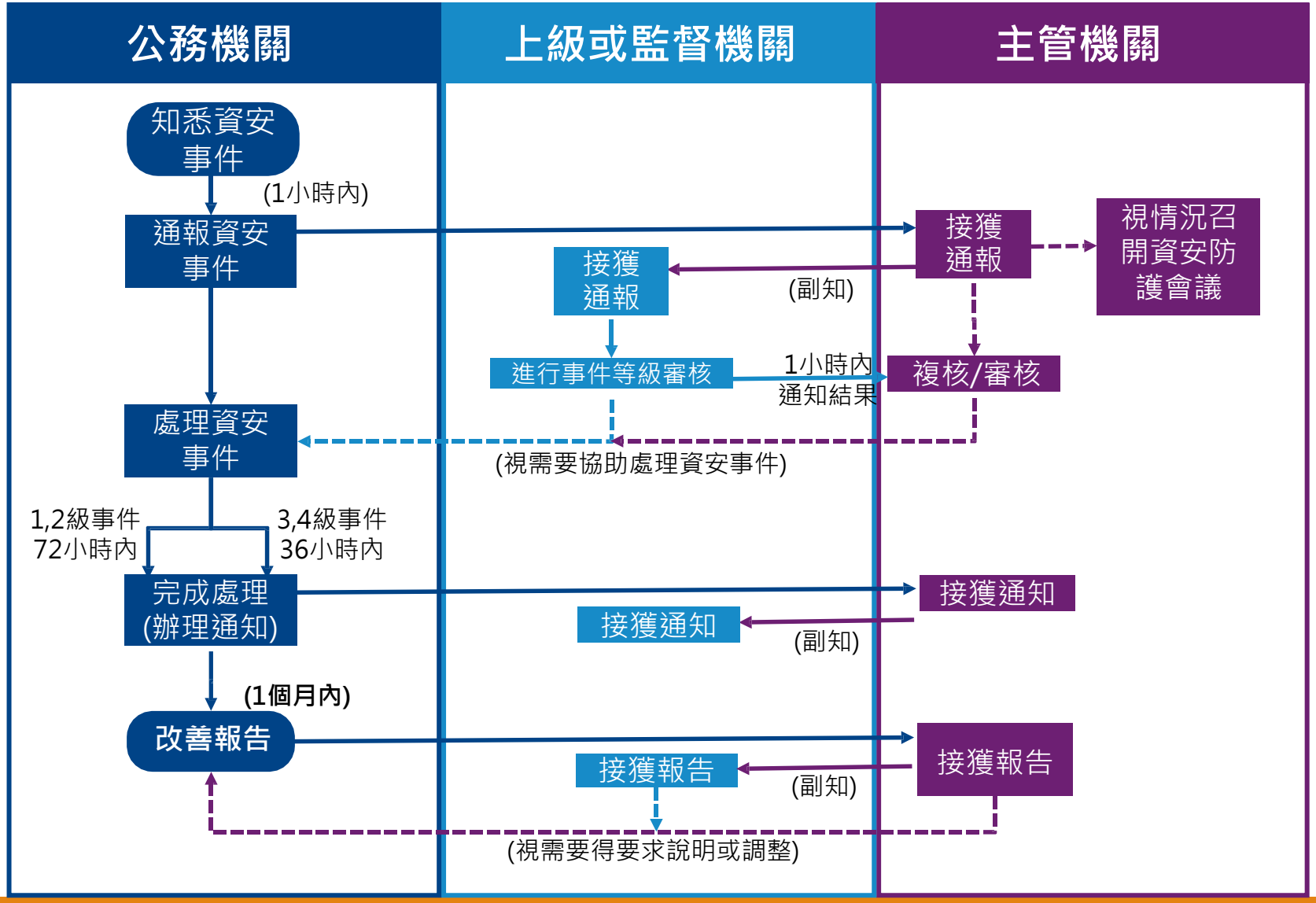
資通安全事件等級分類

事件等級	條件
第一級	一. 非核心業務資訊遭輕微洩漏 。 二. 非核心業務資訊或非核心資通系統遭輕微竄改 。 三. 非核心業務或非核心資通系統之運作受影響或停頓，於可容忍中斷的時間內回復正常運作。
第二級	一. 非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。 二. 非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵 基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改 。 三. 非核心業務或非核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中段時間內回復正常運作。 四. 有前向各款情形之資通安全事件，影響二個以上機關者。

資通安全事件等級分類(續)

事件等級	條件
第三級	一. 未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關建基礎設施維運之核心業務資訊遭輕微洩漏。 二. 未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。 三. 未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。 四. 有前項各款情形之資通安全事件，影響二個以上機關者。
第四級	一. 一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。 二. 一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。 三. 涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。 四. 有前項各款情形之資通安全事件，影響二個以上機關者。

資安事件通報流程-公務機關



行政院頒布各機關資通安全事件通報及應變處理作業程序

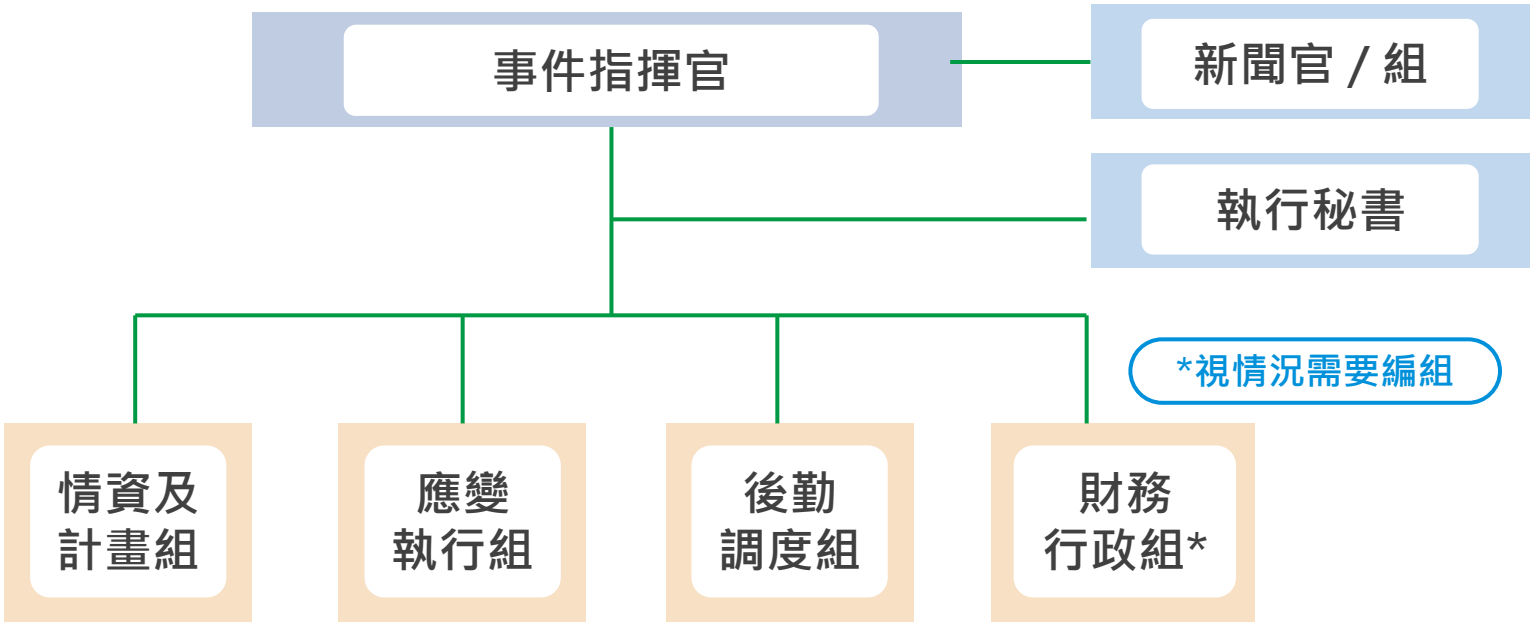
目的

一、為確保資通安全管理法(以下簡稱本法)納管之公務機關及特定非公務機關(以下簡稱各機關)於發生資通安全事件時，依本法及資通安全事件通報及應變辦法相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對各機關業務之衝擊影響，並確保資通安全事件發生時之跡證保存，特訂定本程序。

資通安全事件通報及應變小組

二、各機關應成立資通安全事件通報及應變小組(以下簡稱通報應變小組)，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。

通報應變小組組成建議如下圖：



資通安全事件通報及應變小組權責分工(1/6)

各分組代表：

	第一級、第二級 資通安全事件	第三級、第四級 資通安全事件
事件指揮官	機關資訊(安)單位主管	機關資通安全長
新聞官/組	事件指揮官或其授權人員	
執行秘書	機關資通安全專責人員或 資訊人員	機關資訊(安)單位主管
情資及計畫組組長	機關資通安全專責人員或 資訊人員	機關資訊(安)單位主管或 資通安全專責人員
應變執行組組長	機關資通安全專責人員或 資訊人員	機關資訊(安)單位主管或 資通安全專責人員
後勤調度組組長	機關資通安全專責人員或 資訊人員	機關資訊(安)單位主管或 資通安全專責人員
財務行政組組長	機關財務或秘書單位主管	

資通安全事件通報及應變小組權責分工(2/6)

各分組代表之任務：

事件指揮官

為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及機關新聞官/組。

新聞官/組

視事件需要由事件指揮官或其授權人員擔任新聞官或分組代表，資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息及擬定溝通計畫。

執行秘書

為事件指揮官幕僚，負責督辦通報應變小組各項業務。

資通安全事件通報及應變小組權責分工(3/6)

各分組代表之任務：

情資及計畫組

1. 本分組負責辦理下列事宜：
   (1) 資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查 各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC 等。
   (2) 應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。
2. 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級機關、中央目的事業主管機關或相關機關，亦應視情況或納入政風單位派員參與，以提供必要之支援協助。

資通安全事件通報及應變小組權責分工(4/6)

各分組代表之任務：

應變執行組

1. 本分組負責辦理下列事宜：
   (1)執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度資訊及資通安全人員執行災害搶救及 損害管制，防止次波攻擊及損害擴散。
   (2)復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。
   (3)跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。
2. 本分組由機關資通安全專責人員、資訊人員、業務單位及委外廠商組成，上級機關、中央目的事業主管機關或 相關機關得於機關申請支援時派員參與。

資通安全事件通報及應變小組權責分工(5/6)

各分組代表之任務：

後勤調度組

1. 本分組負責辦理下列事宜：
   (1) 事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。
   (2) 提出改善建議：依據事件調查根因，提出短、中、 長期改善建議。
   (3) 彙整改善報告。
   (4) 撰寫調查、處理及改善報告。
   (5) 追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。
2. 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級機關、中央目的事業主管機關或相關機關得於機關申請支援時派員參與。

資通安全事件通報及應變小組權責分工(6/6)

各分組代表之任務：

財政行政組

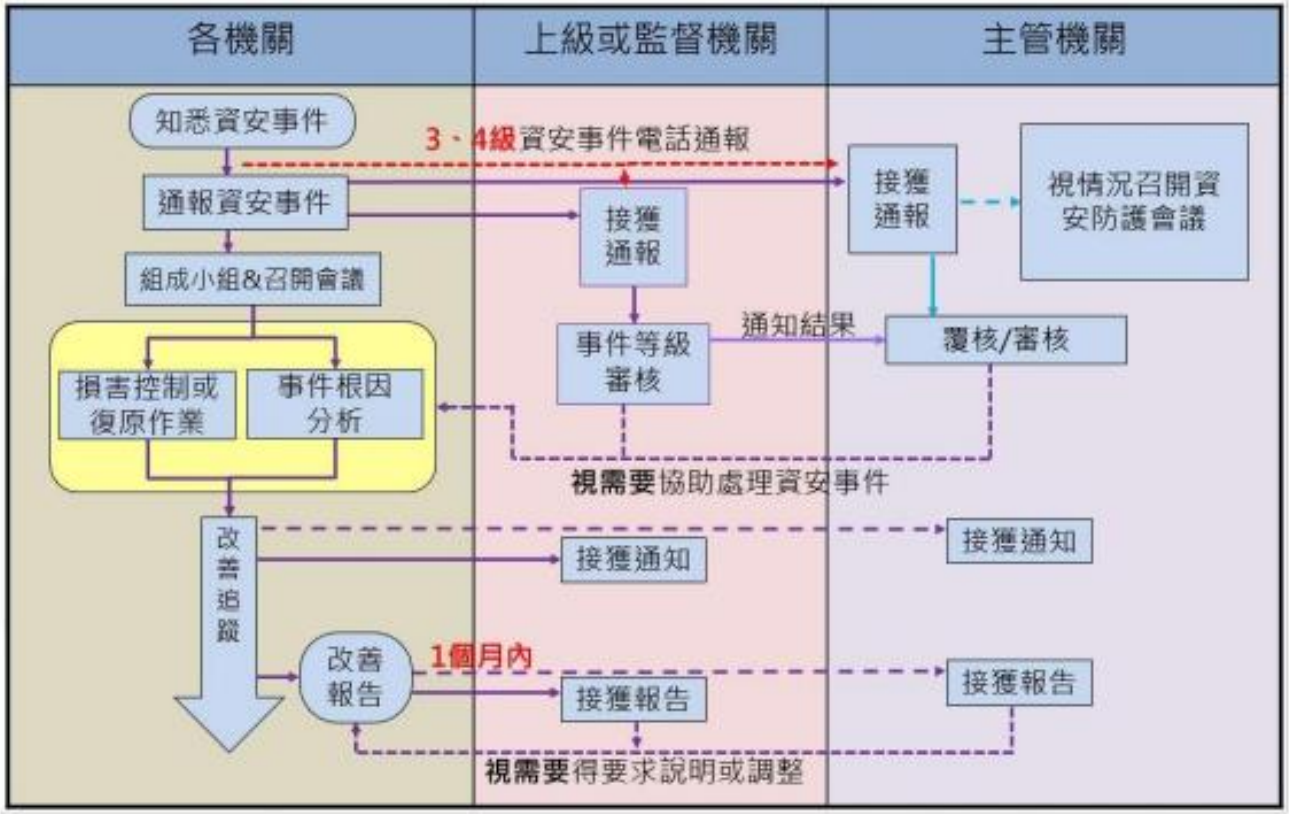
本分組視事件需要由機關財務或秘書單位組成，負責辦理預算調撥及提供行政支援事宜。

小結：

各機關得以現有分組為基礎，依各機關編制及業務分工，經機關資通安全長同意後調整通報應變小組組成及各分組代表，另得視資通安全事件或機關資通環境需要調整各分組任務。

資通安全事件通報及應變處理作業流程

三、各機關之資通安全事件通報及應變程序，應包含通報資通安全事件、**組成通報應變小組**與召開事件應變會議、損害控制或復原作業、事件根因分析及改善追蹤等項目(如下圖)，並依本法施行細則第六條第一項第九款規定納入資通安全維護計畫中。



資通安全事件通報及應變處理作業程序(1/6)

各項程序如下：

(一)

通報資通安全事件

1. 各機關應依本法及資通安全事件通報及應變辦法規定，由情資及計畫組依主管機關或中央目的事業主管機關指定方式完成事件通報。
2. 第三級或第四級資通安全事件，各機關除依前目規定通報外，應另以電話或其他適當方式通知上級機關或中央目的事業主管機關，無上級機關者，應通知主管機關；行政院資通安全處(數位發展部資通安全署成立後為該署)就第三級或第四級資通安全事件，依國土安全緊急通報作業規定轉報行政院國土安全辦公室。

(二)

組成通報應變小組與召開事件應變會議

各機關於完成第三級或第四級資通安全事件之初步損害控制後應召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項，並得視情況邀請上級機關、中央目的事業主管機關或主管機關出席：

1. **資通安全事件概況。**
2. **評估受影響範圍。**
3. **其他必要之討論事項。**

資通安全事件通報及應變處理作業程序(2/6)

(三)

損害控制或復原作業

1. **由應變執行組執行損害控制或復原作業，並辦理下列事項：**
   - ①確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。
   - ②評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。
   - ③於完成損害控制或復原作業後，依主管機關或中央目的事業主管機關指定之方式完成通知作業。
2. **第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項：**
   - ①定時向事件指揮官、通報應變小組成員、上級機關或中央目的事業主管機關回報控制措施成效；無上級機關者，應回報主管機關。
   - ②倘涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。

資通安全事件通報及應變處理作業程序(3/6)

(四)

事件根因分析

由後勤調度組執行，依資通安全事件等級，建議辦理事項如下：

1. 依第四點跡證保存之規定保存相關跡證，**惡意程式建議得請防毒軟體或資安服務公司檢測**，並上傳至Virus Check網(https://viruscheck.tw/)分析，**以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。**
2. 除設備故障外，後勤調度組應依據前目保存跡證，由組長督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如發現惡意程式，應提出惡意程式分析。
3. 依據事件調查根因分析結果，機關應評估短、中、長期 資安管理改善策略，其內容如下：
   - ① **短期**：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。
   - ② **中期**：依據事件根因提出三至六個月內完成之強化作為，例如盤點機關老舊設備，並訂定汰換期程。
   - ③ **長期**：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養機關資安人員能力。
4. 由執行秘書將事件調查根因及改善策略提報事件指揮官裁處，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關；無上級機關者，應送交主管機關。

資通安全事件通報及應變處理作業程序(4/6)

(五)

改善追蹤

各機關進行事件改善追蹤時，應視需要召開會議，並據以辦理下列事項：

1. 評估改善作為期程。
2. 評估執行成效，並據以調整改善策略。
3. 配合上級機關、中央目的事業主管機關或主管機關辦理相關改善作為。
4. 第三級或第四級資通安全事件，應由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善 措施為止，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關；無上級機關者，應送交主管機關。
5. 依**主管機關或中央目的事業主管機關指定之方式**，送交調查、處理及改善報告；第三級或第四級資通安全事件， 應另以密件公文將該報告送交主管機關及上級或監督機關。
6. 機關送交調查、處理及改善報告後，相關改善事項應納入機關現行定期追蹤管考機制。

資通安全事件通報及應變處理作業程序(5/6)

四、跡證保存

為確保資通安全事件發生時，各機關所保有跡證足以進行事件根因分析，各機關依**資通安全事件等級**，建議辦理下列事項，並應視事件情形辦理其他必要之跡證保存事項：

1

各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌(log)，並**建議定期備份至與原稽核系統不同之實體系統**，其保存範圍及項目如右表。

註:若資訊系統已向上集中者，則可由上級機關保存。

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

資通安全事件通報及應變處理作業程序(6/6)

2

發生資通安全事件時，機關應依下列原則進行跡證保存：

1. 機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。
2. 若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。
3. 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。
4. 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

3

各機關於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中明定紀錄保存及備份規定。

資安事件緊急應變處理方式

資安事件處理方式

- 制訂資安事件處理機制，事先找出潛在的問題，避免事件擴大成危機
- 在資安事件發生之初，投入適當的資源，以管理事件
- 儘量控制或減少對校方的風險
- 適當的處理各種抱怨

43

應變處理定義

- 應變處理是提供有效的程序，解決或緩解已發生的資通安全事件
- 異常行為事件本身即是一種複雜資訊處理活動，當資安事件發生，時間即是應變處理的挑戰
- 應變處理強調在日常的準備與規劃

44

危機事件管理

- 危機預防階段
  - 危機偵測
  - 危機防範
  - 研擬各種應變計畫
- 危機處理階段
  - 判定危機本質
  - 設立危機處理目標
  - 執行危機處理計畫
- 復原階段
  - 擬訂重建復原計畫
  - 召開檢討會議
  - 回到危機預防階段

45

危機事件的特徵

- 意外
- 訊息混亂
- 事件影響逐漸升高
- 失去控制
- 來自內部/外部嚴重關切
- 開始產生精神折磨
- 恐慌
- 需要公開化解疑慮

46

危機處理考慮的優先順序

- 保護家長與學生的權益
- 學校的形象
- 業務持續運作

47

對外說明原則

“

#對外說明原則

- 只有授權的發言人，才可對外說明
- 強調首要目標為保護家長、學生或老師的權益
- 說明時必須快速與所有聽眾有目光接觸
- 說明時必須平衡校方事件處理方式與可能的法律問題
- 說實話，避免回答假設性的問題或缺乏事實根據的話
- 報告主管機關（不要透過媒體）
- 儘快提供最新的資訊，以滿足與引導媒體
- 由最高主管作對外危機說明

說明方式

“

說明方式

誰該說明

- 只有授權的發言人，才可對外說明

說明什麼

- 只能說明事先經過核准的事實

哪些不該說

- 未經核准的資訊不能說
- 不要傳播謠言或推測的話
- 不要指責或歪曲事實

危機溝通的原則

- 釐清事件的真象
- 決定何時可以宣佈何種消息
- 儘快將可以公佈的訊息告知媒體
- 當機立斷立即處理
- 反應坦白而開放
- 持續不斷的進行溝通
- 重新提昇受損的形象

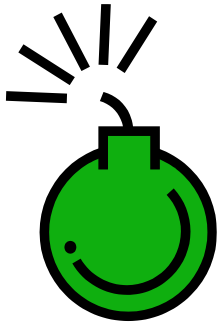
營運持續基本觀念與實作

可能造成營運中斷的風險

停電

水災

重大傳染病



爆炸

駭客攻擊

供應鏈中斷

法定中止

建築物損壞

火災

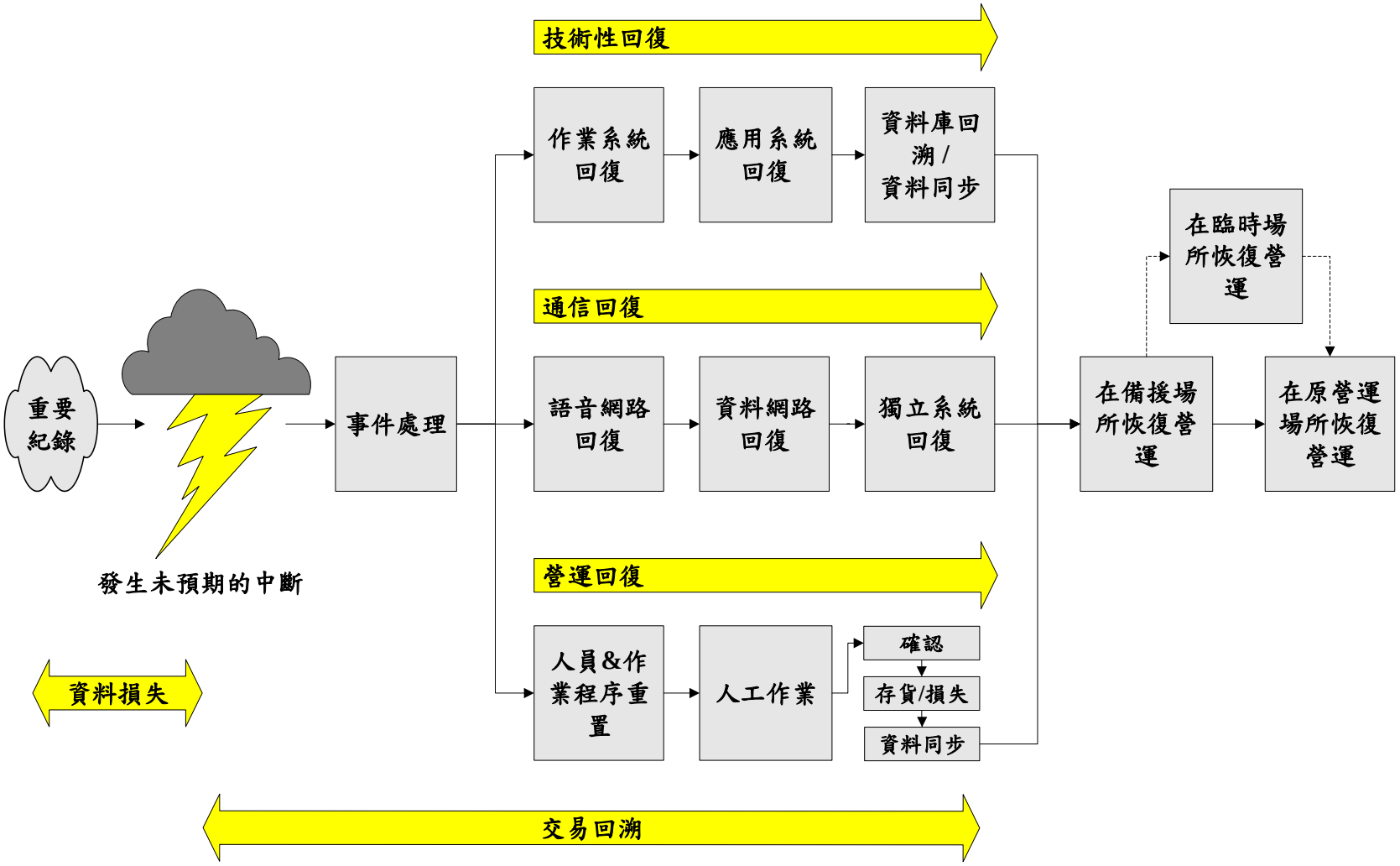
設備故障

資安事件管理與營運持續管理間的關係

營運持續概念

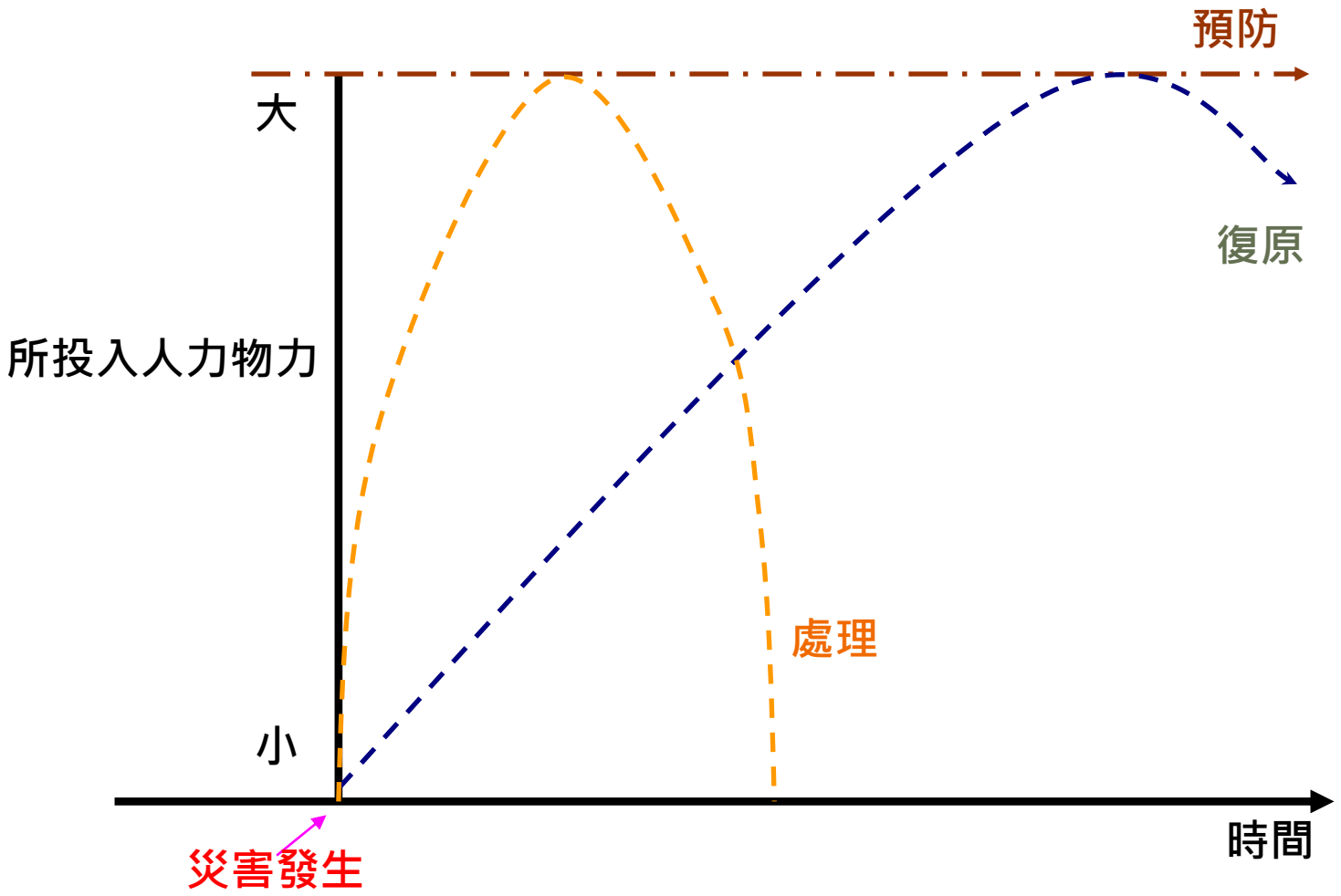
54

營運持續概念(續)


技術性回復
作業系統回復
應用系統回復
資料庫回溯/資料同步
通信回復
重要紀錄
事件處理
語音網路回復
資料網路回復
獨立系統回復
在臨時場所恢復營運
在備援場所恢復營運
在原營運場所恢復營運
發生未預期的中斷
營運回復
人員&作業程序重置
人工作業
確認
存貨/損失
資料同步
資料損失
交易回溯

55

營運持續作業主要階段



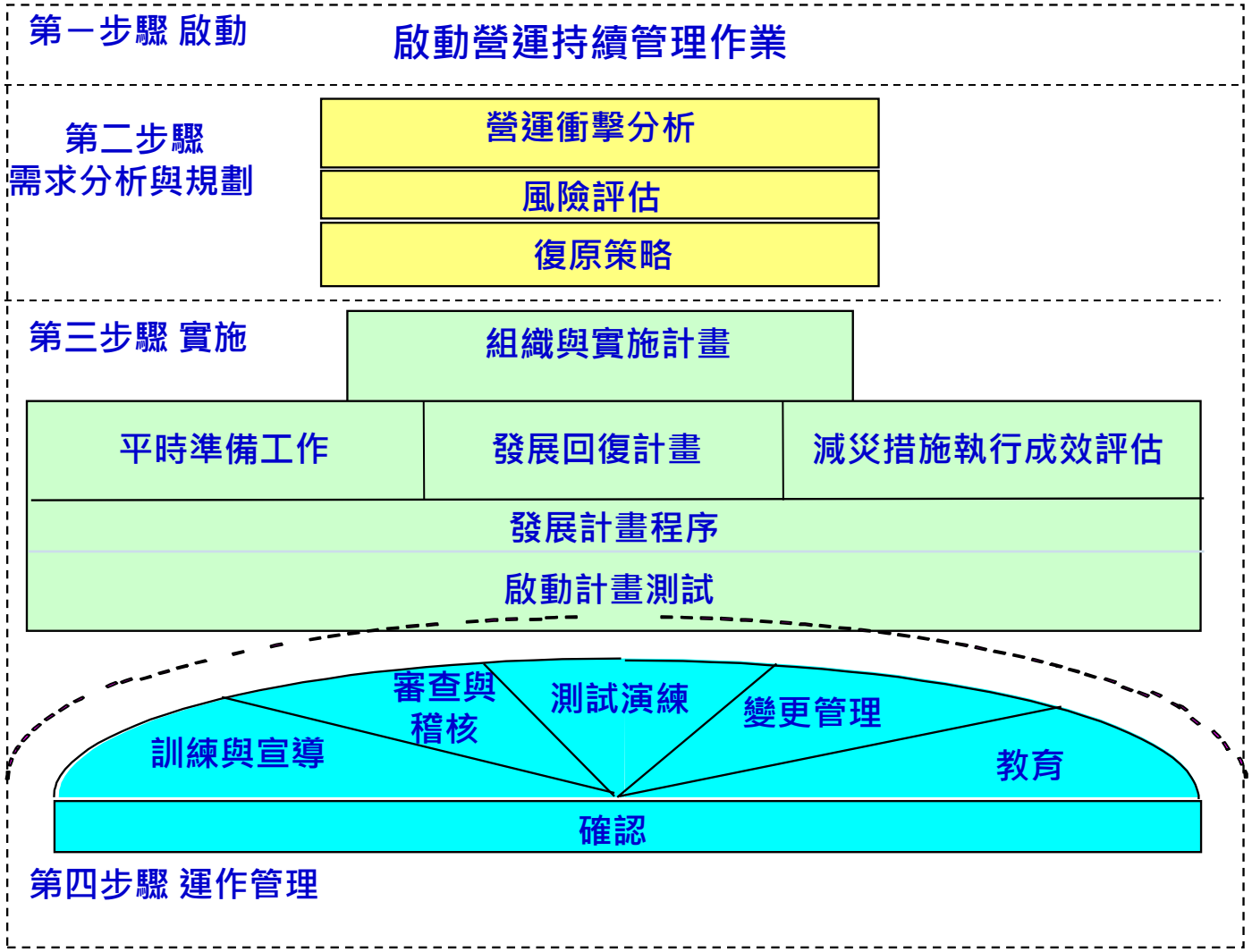
56

災害發生第一要務

- 第一優先—『人員生命安全』
- 在任何情形下絕對不要讓人員冒風險，當重大風險發生立即疏散人員

57

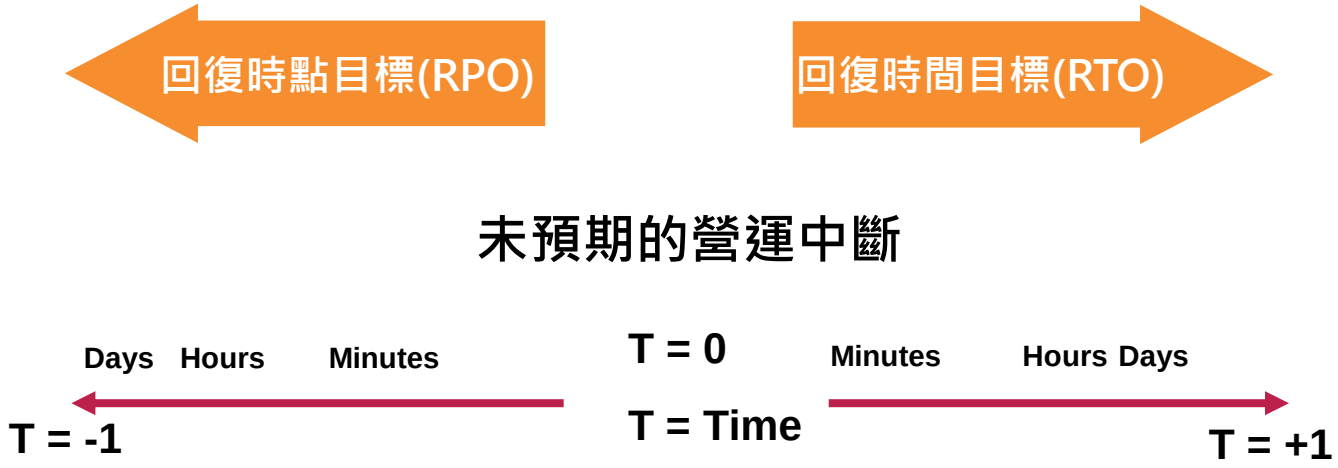
營運持續管理流程


第一步驟 啟動
啟動營運持續管理作業
第二步驟
需求分析與規劃
營運衝擊分析
風險評估
復原策略
第三步驟 實施
組織與實施計畫
平時準備工作
發展回復計畫
減災措施執行成效評估
發展計畫程序
啟動計畫測試
審查與
稽核
測試演練
變更管理
訓練與宣導
教育
確認
第四步驟 運作管理

58

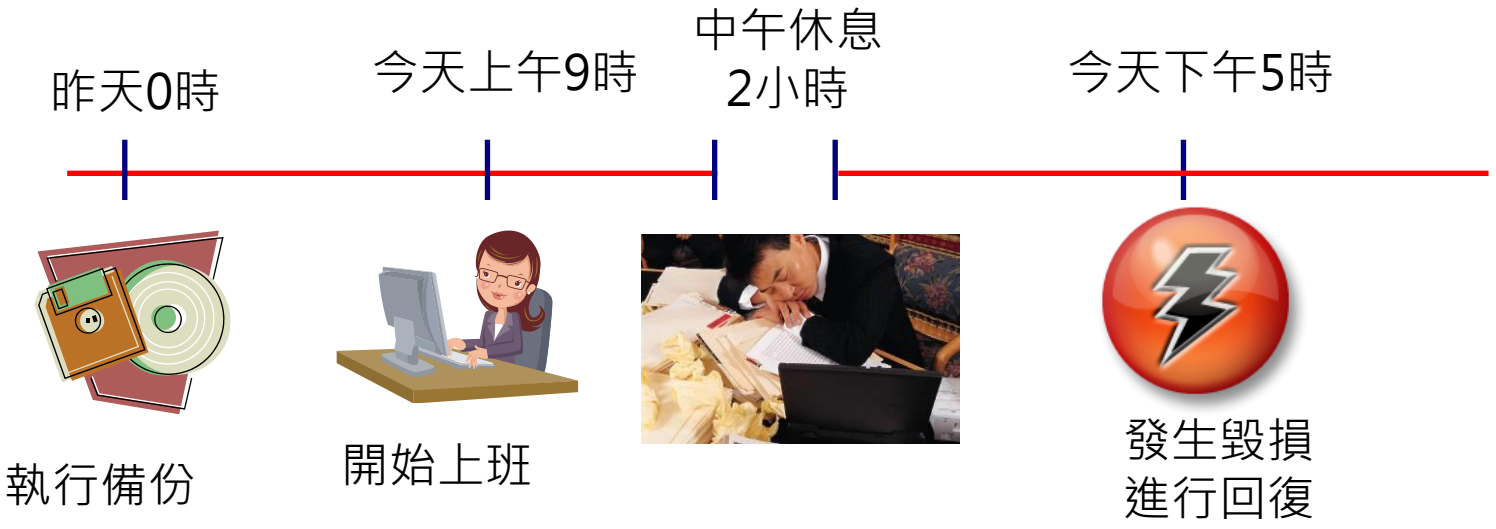
營運持續管理3大重要指標

- MTPD (Maximum Tolerable Period of Disruption)最大可容忍中斷時間
- RTO (Recovery Time Objective)回復時間目標
- RPO (Recovery Point Objective)回復時點目標



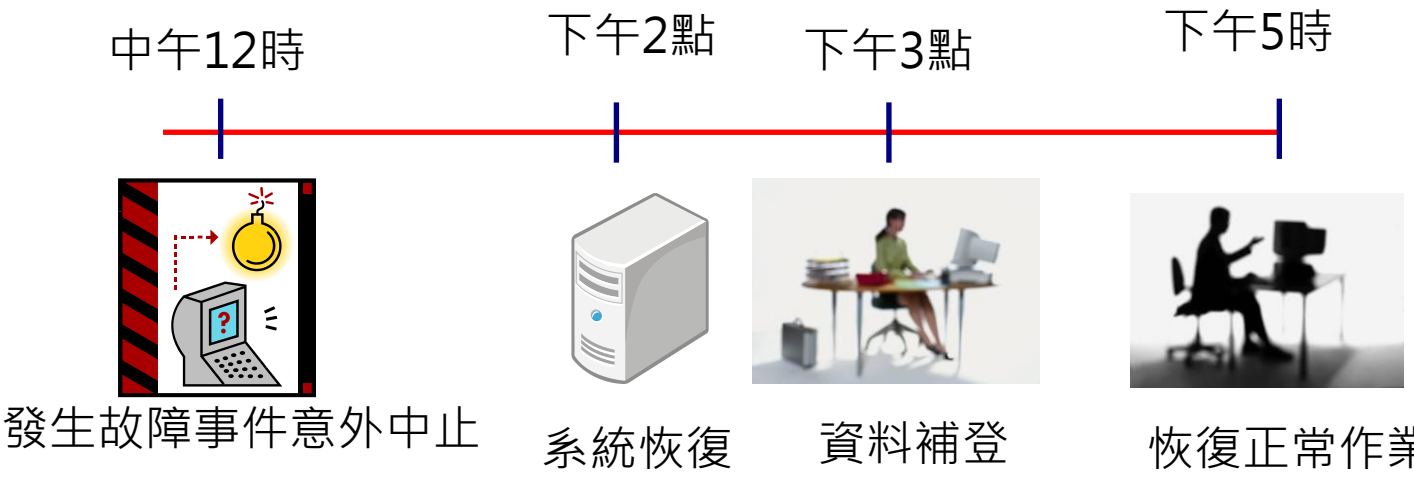
RPO的意義

- RPO (Recovery Point Objective)回復時點目標
- 以下圖為例：
  - 回復資料為前一天的資料
  - 資料最大可能損失為(17-9-2)+1=7小時，此即為其RPO值



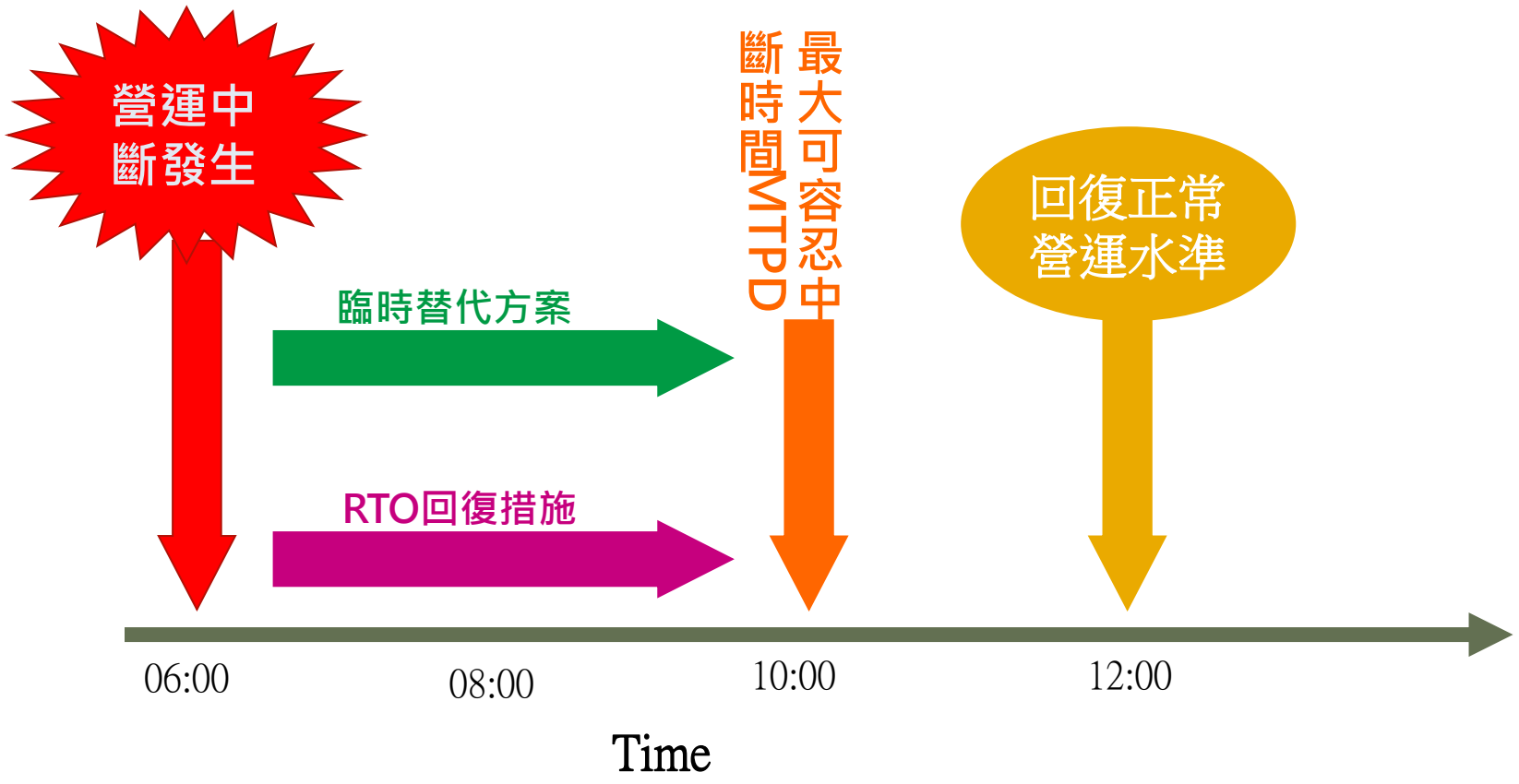
RTO的意義

- RTO (Recovery Time Objective)回復時間目標
- 以下圖為例：
  - 故障發生於中午12點，等系統恢復及資料補登至中斷時間為止，才算完成復原
  - 故17-12=5小時，此即為其RTO值



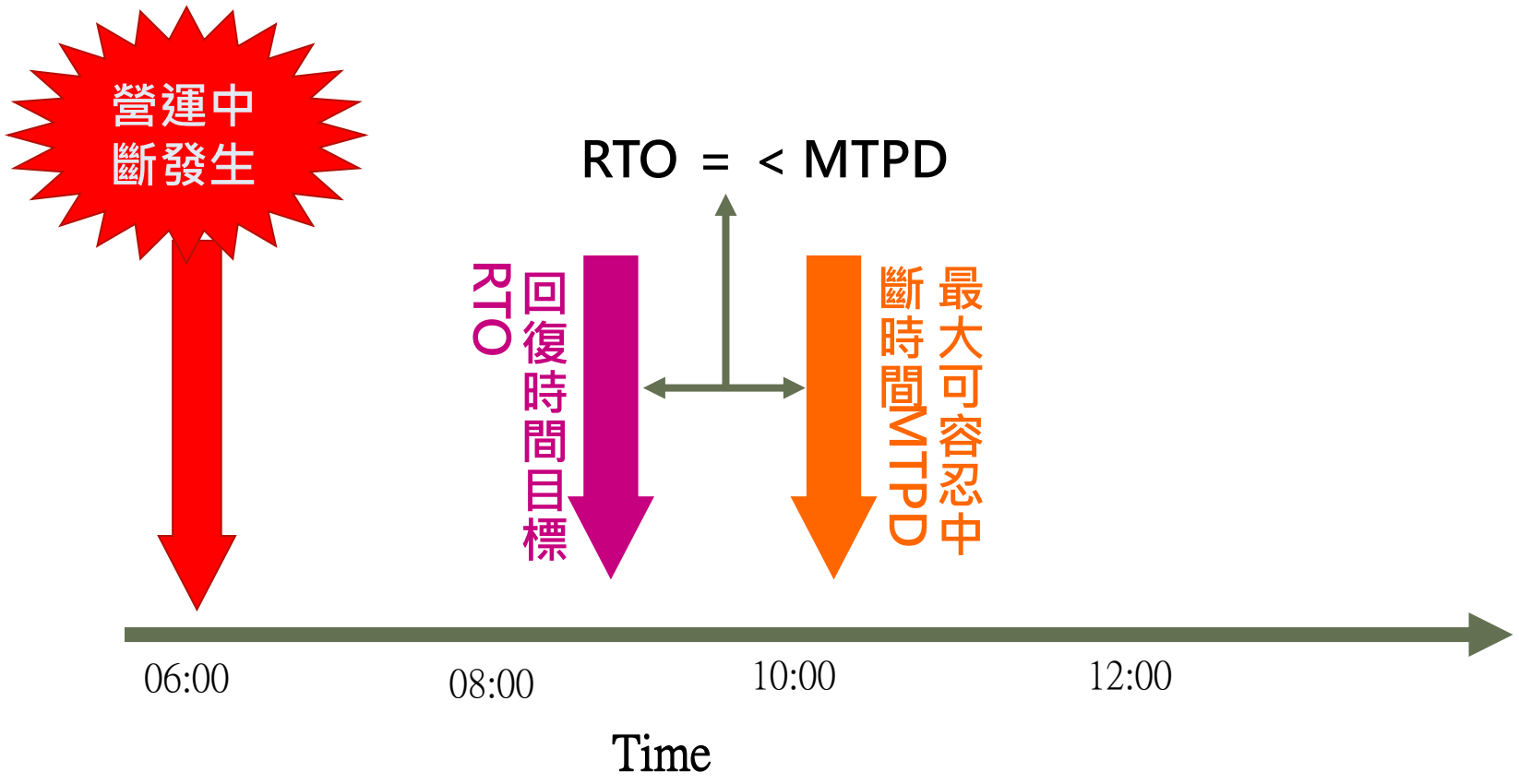
MTPD與RTO關聯示意圖(一)

- 思考營運持續管理措施要從”Worst Case”出發，如此才會充分考量到中斷事故所帶來之最大損害

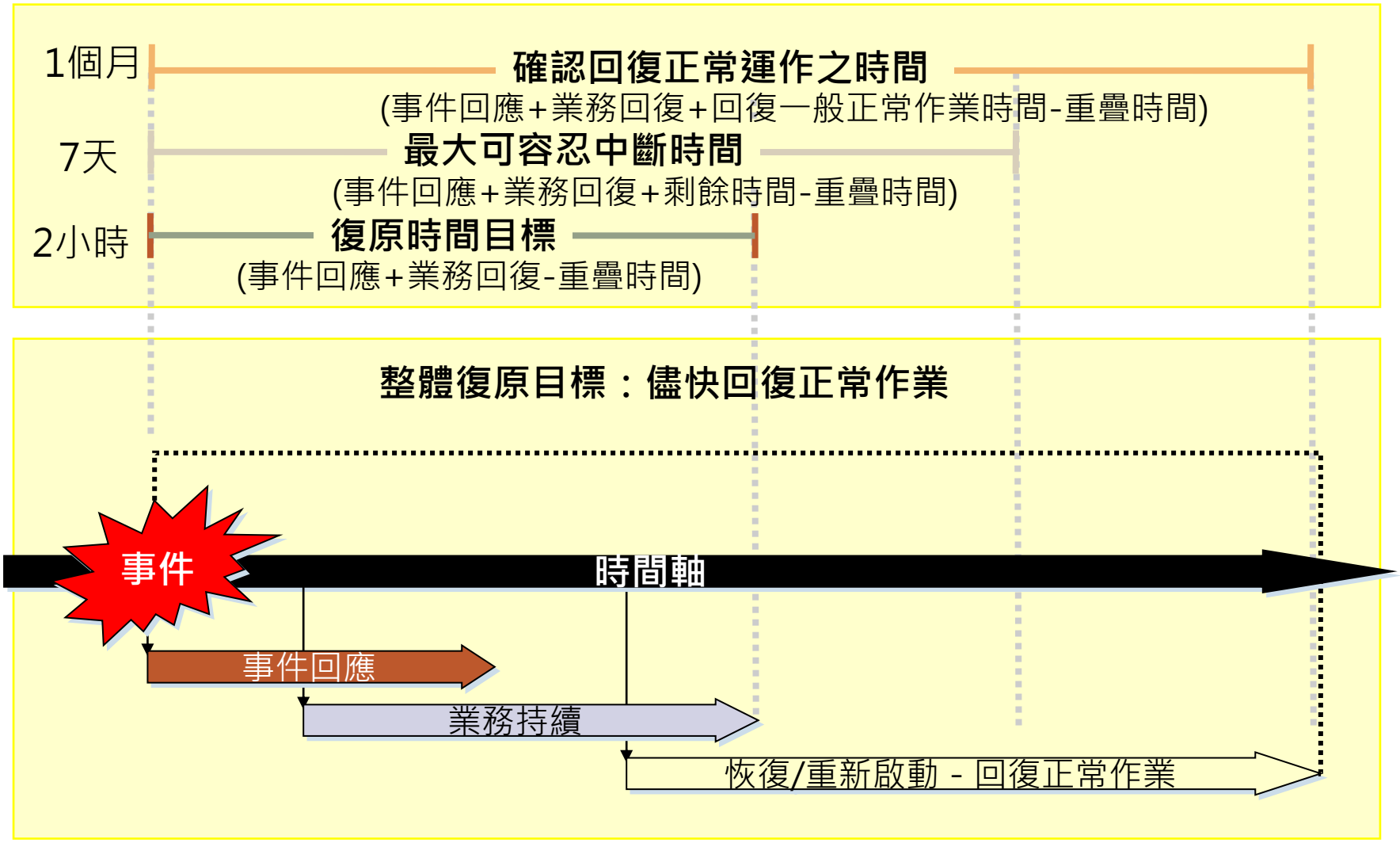


MTPD與RTO關聯示意圖(二)

- 回復時間目標(RTO)=執行營運持續計畫恢復業務所需要的時間



MTPD與RTO的關係性



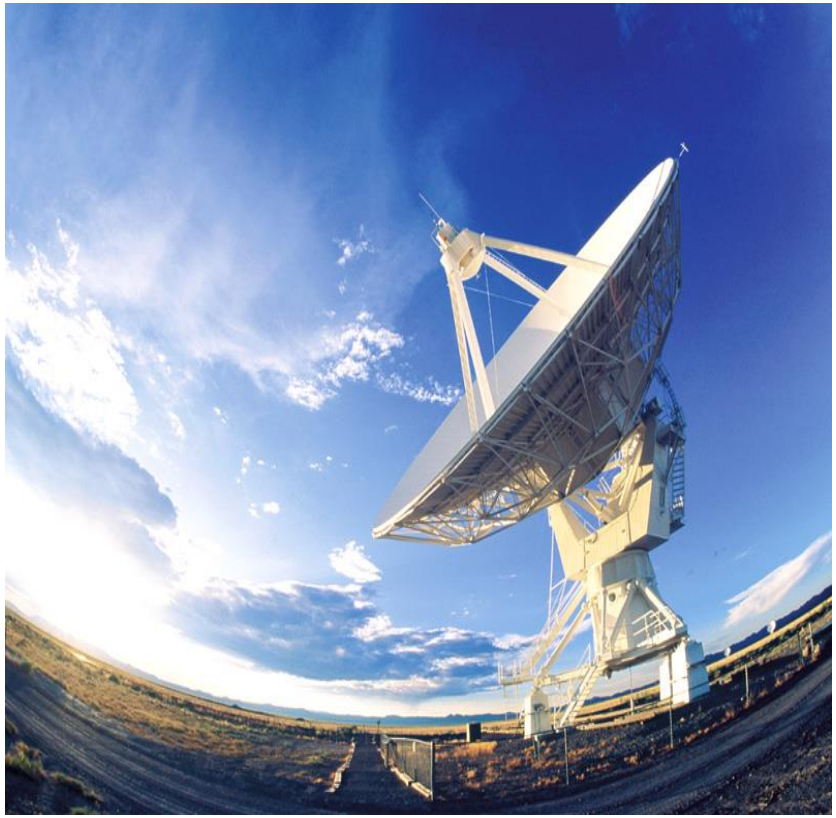
營運衝擊分析

- 以業務流程為主

業務名稱	MTPD	RTO	RPO	相關資源 (人/系統/硬體)	影響

影響的種類

- 財務
- 家長或供應商
- 公共關係/商譽
- 法律
- 法規/合約要求
- 環境
- 營運
- 人員
- 主管機關



66

相關資源

- 技術性資源 - 技術文件、表單
- 連線設備
- 資料/媒體
- 外部資源(廠商、公用設施)
- 內部服務與資源
- 辦公設備
- 空間
- 人員
- 特殊設備
- 通信

學校資安維護計畫(核心業務)

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
教務業務	無	■為本機關依組織法執掌，足認為重要者	學校教學業務作業無法運作	8小時
學生事務業務	無	■為本機關依組織法執掌，足認為重要者	學校學生事務業務作業無法運作	8小時
總務業務	無	■為本機關依組織法執掌，足認為重要者	學校總務業務作業無法運作	8小時
輔導業務	無	■為本機關依組織法執掌，足認為重要者	學校輔導業務作業無法運作	8小時
幼兒教育業務	無	■為本機關依組織法執掌，足認為重要者	學校幼兒業務作業無法運作	8小時

學校資安維護計畫(非核心業務)

非核心業務	業務失效影響說明	最大可容忍中斷時間
人事業務	人事業務無法運作	24小時
會計業務	會計業務無法運作	24小時

營運持續運作計畫架構

計畫架構

- 應建立及維持單一的持續作業計畫架構，使各種不同層次及等級的計畫相互連貫，並應訂定測試計畫及維護計畫之優先順序
- 每項業務之持續運作計畫，應明定行動之條件，以及員工執行計畫之責任；組織研擬新的資訊計畫，應與緊急應變計畫程序相一致（例如疏散計畫、現有應用系統的備援作業安排，以及通信及空間的配置）
- 在業務持續運作管理之整體架構內，應訂定不同層次及等級的計畫，每一層次及等級的計畫，應涵蓋不同的計畫重點及負責回復作業的人員安排

營運持續運作計畫內容

- **業務持續運作計畫，應考量的作業程序如下：**
  - 訂定緊急應變作業程序，規定如何在發生危害組織業務運作或危及生命的重大事件發生時，應立即採取的行動
  - 訂定備援作業程序，規定如何將必要的組織業務活動或是支援性的服務，移轉至另外一個備援/臨時的作業地點
  - 訂定回復作業程序，規定如何採取回復作業，使組織業務回復到原來正常的業務運作
  - 訂定測試作業程序，規定如何及什麼時間執行測試作業
- **緊急應變作業、人工備援作業及回復作業計畫等，應指定適當的單位或人員負責**

BCP演練方式

複雜度	演練方式	流程	目的	最佳實務建議頻率
簡易	沙盤推演	覆核與改善內容 挑戰BCP的內容	更新/確認有效性 稽核/證明符合性	至少每年一次 每年進行
中等	走位式演練	挑戰BCP的內容	包含彼此的互動與確認參與者的角色	每年進行
	模擬	使用假設的情境確認BCP內容已包含必要資訊與成功的回復	合併相關計畫	每年進行或一年兩次
	演練關鍵活動	在一個可控制的狀況下啟動，不對營運造成損害	在固定時間內於異地進行作業	每年進行或更少
複雜	演練全面的復原演練計畫，包含事件管理	包含建築物 / 全區域的演練	確認業務持續運作計畫內容正確性	每年進行或更少

Source: BS25999-1

BCP更新的時機

- **納入計畫更新之事項如下：**
  - 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
  - 組織及人員地址及電話號碼的變動
  - 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

建立BCP變更機制

- 應指定專人負責BCP計畫變更事宜，個別計畫原則上至少每一個月要檢查評估一次，完整的計畫至少應每年檢討評估一次
- 應建立BCP計畫變更的控制機制，以確保BCP計畫變更前，以及賦予員工相關責任前，能將相關的訊息告知相關人員

問題與討論