新北市政府教育局

行政院管考系統填報
教育訓練

講師：葉益禎

中華民國112年3月28日

課程大綱

序號	大綱
一	近期重大個資事件分析
二	資通安全管理法及其子法簡介
三	資通安全維護計畫實施情形填報注意事項
四	問題與討論

近期重大個資事件分析

案例一、微風集團事件概述

微風集團遭竊90萬筆個資 勒索金額曝！駭入時間精準疑有內鬼

微風集團內部資料遭駭，近日收到匿名網路勒索信件，已於第一時間啟動損害機制，目前內部資安團隊已完成軟體以及作業系統安全性更新，微風並指出，經清查確認，外流個資與公司資料庫有落差，因此駭客未必是從微風駭入；微風也提醒會員定期修改密碼，以保障個資安全，避免遭不當利用。

事件經過

在駭客論壇BreachForums，有人發文聲稱竊得微風百貨的內部資料，內容包含所有的業務資料、公司及供應商的資料、90萬用戶個資、發票、訂單、付款資料，以及30個專案的原始碼，檔案大小超過150 GB，駭客更強調個資含有會員的帳號及密碼。

微風則表示，近日有收到匿名網路勒索信件，向微風集團勒索3個比特幣（折合台幣222萬5千餘元）買回這批會員個資。

處理過程

- 網路勒索信件，向微風集團勒索3個比特幣，微風集團經內部討論後決定不歹徒妥協，先向行政院數位發展部報備，再向刑事局偵九大隊報案提告妨害電腦使用等罪。
- 微風集團15日報案當天也同步對外發表聲明，表示集團將會全面更新系統，系統更新過程將暫時暫停會員點數活動，微風集團允諾加強系統安全並全面要求會員修改登入帳密，以維個資隱私安全。

圖:聯合報

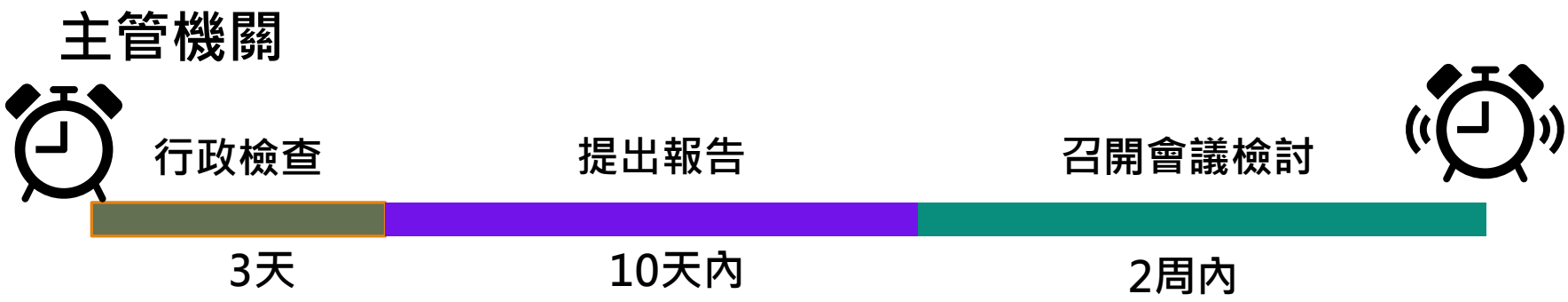
疑似入侵管道

資料參考來源 : 上報Up Media、中天新聞網

- 駭客從境外入侵電腦 : 駭客使用位於香港的IP登入位置發送恐嚇電郵，也曾多次利用位於瑞士的網路惡意登入微風集團的商務平台伺服器
- 不排除有內神通外鬼 : 發現駭客在15日準確利用微風集團商務平台系統全面更新維護的作業時間，精準地進入系統後台連線，竊取該集團逾90萬筆會員資料及20多個公司商業營運發展專案，利用高速網路在數小時內成功下載，檢警認為駭客抓準被害公司系統全面維護更新，防火牆暫時關閉期間發動網路攻擊，不排除有內神通外鬼情事。

目前處理狀況

- 依個人資料保護法規定，本案主管為經濟部，資安院已經配合經濟部商業司前往微風百貨進行行政調查，將針對微風百貨的資安措施進行專業分析與鑑識技術等協助
- 調查本案業者原先所採取的資通系統防護措施，分析造成疑似個資外洩的原因，並提出後續相關強化作為建議，做為主管機關提供業者參考，防止類似事件再度發生。



微風集團違反法令

個人資料保護法

第二十七條第一項

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第二十七條第二項

中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

罰則

- 依個人資料保護法第48條第4款規定，違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。可處新臺幣二萬元以上二十萬元以下罰鍰

案例二、 iRent 事件概述

和泰 iRent 用戶10萬個資遭流出，機敏資料門戶大開

國外一名安全研究員 Anurag Sen 發現，和泰集團旗下共享汽機車服務 iRent 其中一組雲端資料庫沒有加密保護，任何知道該資料庫 IP 位址的人都可存取 iRent 用戶姓名、手機、電子郵件、地址、基過base64編碼之圖檔，以及部分信用卡資訊等機敏資料。

事件經過

根據資料庫搜尋引擎 Shodan 紀錄顯示，該資料庫資料量高達 4.2TB，存放於和泰汽車的雲端伺服器中，且並未受到密碼保護，任何使用者只要知道IP地址，即可進入資料庫查詢3個月內知會員異動資料，而網路瀏覽器Shodan數據顯示，該資料庫約從2022年5月就開始洩漏資料，直到2023年1月才被發現，國外研究員於 1/28 日發送電子郵件通知和泰汽車，然而卻未收到回應，且該資料庫還在持續更新。

處理過程

- 外媒聯絡數位發展部，部長唐鳳得知後第一時間將此事轉由「台灣電腦網路危機處理際協調中心(TWCERT/CC）」處理，讓資料庫無法進入。
- 和泰汽車證實知悉資料外洩，並立即切斷該資料庫IP的外部連接，將再次對主機系統做弱點及滲透掃描，並確保用戶交易過程全程採加密，以及導入ISO27701隱私資訊管理系統，加強資安防護。

圖片來源：聯合新聞網 2023.02.02

iRent 事件剖析

兩大資料庫缺失

存取權控制失效

未設置存取權限，導致任何人都能連線進入資料庫。

資料處理不當

未對機敏資料進行**去識別化**，導致用戶真實資料外洩。

事件回應與影響

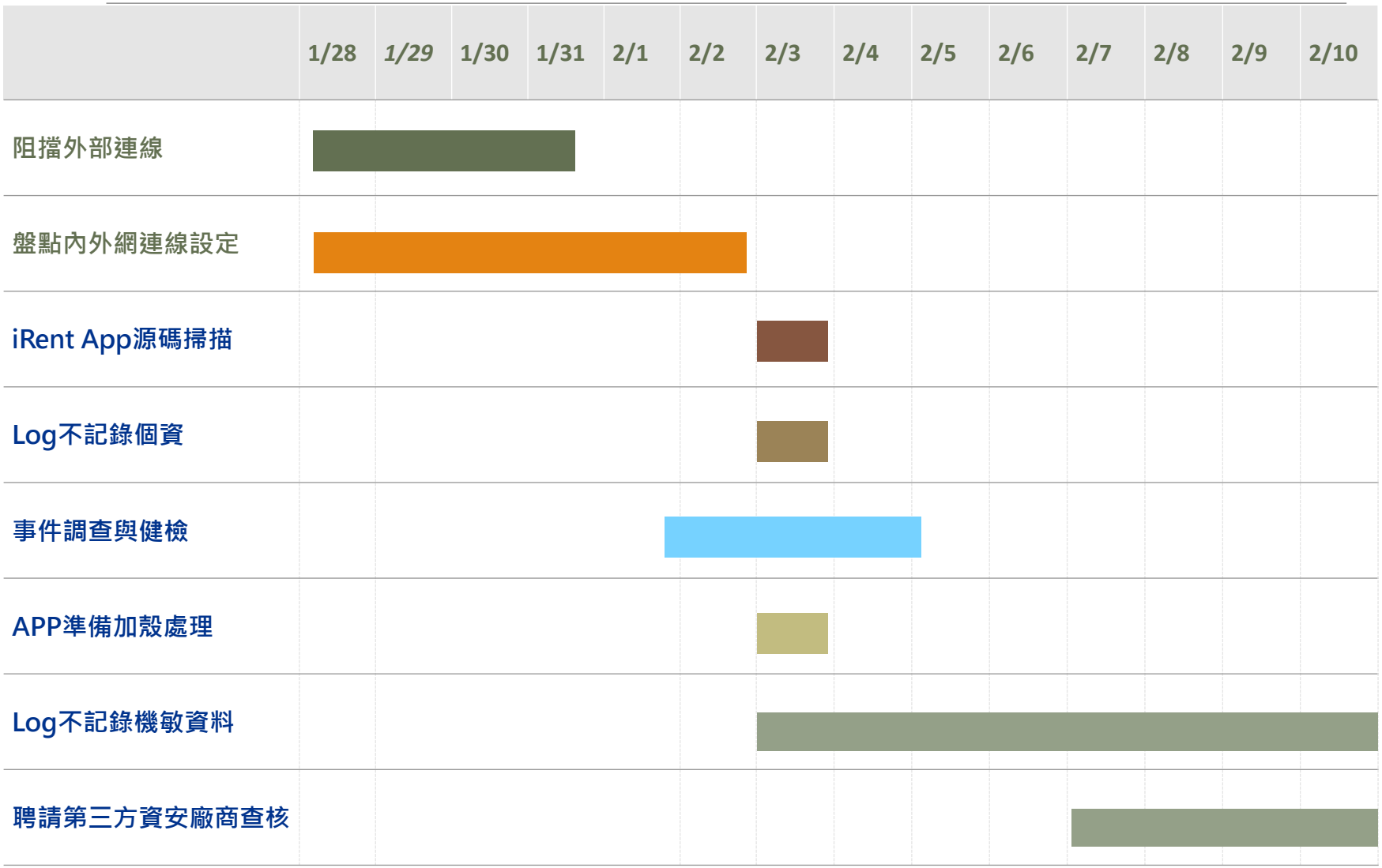
和泰回應

- 和泰汽車表示經查發現為紀錄應用程式 Log 檔之「**暫存資料庫**」出現漏洞，外部資訊人員可能使用特定方法進入該資料庫內查詢近三個月的會員異動資料。
- 可能受影響會員資料約有 14 萬筆，包括會員姓名、電話、地址、經遮蔽保護的部分信用卡資訊。將儘速針對可能受影響之用戶寄發通知與補償，提醒用戶留意潛在詐騙風險。

事件影響

- 該資料庫未加密已長達9個月，難保無人發現這些資料，若曾遭惡意駭客存取，可能引發釣魚郵件、信用卡盜刷等相關風險。
- 台北市區監理所發函要求和雲行動服務股份有限公司，於2月2日前提報其**消費者個人資料檔案安全維護計畫**，並於2月3日前對事件進行說明並提供佐證資料，並要求該公司依個人資料保護法改正完成，屆期未改正則依個人資料保護法按次處2萬元以上20萬元以下罰鍰。

iRent 事件處理流程整理



iRent事件違反法令

個人資料保護法

第二十七條第一項

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第二十七條第二項

中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

汽車運輸業個人資料檔案安全維護計畫及處理辦法

依個人資料保護法第二十七條第三項規定訂定之，汽車運輸業應根據個人資料檔案安全維護計畫及處理辦法之規定訂定安全維護計畫及通報措施

罰則

- 依個人資料保護法第48條第4款規定，違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。可處新臺幣二萬元以上二十萬元以下罰鍰
- 公路總局稽查情形，確認iRent未依「個人資料保護法」與「汽車運輸業個人資料檔案安全維護計畫及處理辦法」採行是當安全措施，且未訂立完整維護計畫，至個人資料洩漏達40萬筆，依法處最高**罰鍰新台幣20萬**元

iRent事件交通部公路總局委外查核結果

援引法條		稽核發現
汽車運輸業個人資料檔案安全維護計畫及處理辦法	第七條第2項 業者應自前項事故發生或知悉時起**七十二小時內**填具個人資料侵害事故通報與紀錄表通報該主管機關，副知交通部公路總局，**未於時限內通報者，應附理由說明之**；並自處理結束之日起一個月內，將處理方式及結果報備查。	和雲行動服務公司個人資料侵害事故通報與紀錄表，未於個資外洩知悉後起七十二小時內通報，且**尚未說明逾時通報原因**，相關通報表單亦無權責主管(如代表人)核准紀錄。
	第三條第1項 保有消費者個人資料筆數達**一百筆以上之業者**，應依本辦法規定，規劃、訂定、修正與執行**消費者個人資料檔案安全維護計畫**（以下簡稱本計畫），其內容應包含第四條至第二十二條規定之相關組織及程序，以落實個人資料檔案之安全維護與管理，防止被竊取、竄改、毀損、滅失或洩漏。	經查業者**尚未訂定**消費者個人資料檔案安全維護計畫，恐不利舉證消費者個資妥善維護處理，有礙健全經營之虞。

iRent事件交通部公路總局委外查核結果

援引法條		稽核發現
汽車運輸業個人資料檔案安全維護計畫及處理辦法	第十八條第1項 業者使用資通系統蒐集、處理或利用消費者個人資料達一百筆，且具對外電子商務服務系統者，應採取下列資料安全管理措施： 一、使用者**身分確認及保護**機制。 二、個人資料顯示之**隱碼**機制。 三、網際網路傳輸之**安全加密**機制。 四、個人資料檔案及資料庫之**存取控制與保護**監控措施。 五、防止外部網路**入侵**對策。 六、非法或異常使用**行為之監控**與因應機制。	經查未發現對外電子商務服務系統執行「防止外部網路入侵對策」及「非法或異常使用行為之監控與因應機制」等情境之定期進行演練及檢討改善紀錄。

交通部公路總局委外查核結果

援引法條	稽核發現
汽車運輸業個人資料檔案安全維護計畫及處理辦法 **第二十一條** 業者應採行適當措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所訂計畫之執行情況；其相關紀錄之**保存期限至少為五年**。	系統日誌原先紀錄**僅留存7日**，尚未發現iRent APP 與iRent租賃系統日誌調整符合五年之紀錄。

經檢視本案對外聲明稿，尚未包含當事人行使權利方式及事件聯繫管道，建議和雲行動服務公司更新聲明稿說明。

交通部公路總局委外查核結果

要求受稽方補充之資料

1. Hims-2-007 **存取控制管理機制**，以確認權限管控情形。
2. iRent **個資盤點表**，以確認個資落實盤點管控。
3. **外部稽核證書**(或驗證通過證明書)，以確認27001、27701驗證範圍包含 iRent APP、 iRent 租賃系統開發生命週期及對客戶提供之服務流程。
4. 內部會議紀錄，以佐證代表人、管理人參與及投入對**事故善盡個資保護**之義務。
5. 數聯資安**事故調查報告**。
6. 精誠/宏碁/果核查驗驗證結果。
7. 雲端儲存位置位於新加坡佐證資料。

iRent 事件精進措施

事前

1. 使用安全資料雜湊演算法如 SHA-256,SHA-384等，確保資料安全
2. 資料庫位置使用非公開IP，阻絕不明外部存取要求
3. 依主管機關規定擬定相關個資安全維護計畫資料
4. 監控資料庫活動，以便及時發現異常流量
5. 確實執行與管理ISO27001,27701等資安制度要求，增強防護

事中

1. 事故發生後立即填寫侵害通報與紀錄表，通報主管機關
2. 立即發布聲明稿，向用戶說明事件緣由及防護措施
3. 確認有無其他系統存在風險

事後

1. 確認事故影響範圍，避免災情擴大
2. 檢討資料安全管理措施，擴大與第三方資安廠商合作
3. 擬定完善諮詢管道及用戶補償措施，提醒用戶可能風險
4. 導入EDR、MDR等防護機制，加強端點防護

案例三、格上 Go Smart 事件概述

格上租車共享車服務 App 出租單洩漏風險

格上租車於2023年2月2日接獲交通部公路總局通報，其共享車服務「Go Smart app」疑似個資外洩，用戶於app提交訂單並完成付款後取得的出租單可透過專業技術取得。

事件經過

出租單為用戶付款後系統自動產出並儲存於 GCS(Google Cloud Storage) ，個資欄位包含姓名、電話、住址、身分證字號及出生日期，該起洩漏風險事件原因為GCS系統設定瑕疵，導致惡意者可透過專業技術取得出租單資料，該項功能於2022年5月上線，至今受影響個資筆數約為1.6萬筆。

處理過程

- 格上租車於接獲通知後一小時內關閉GCS共享車出租單連結，關閉除管理者之外任何人取得出租單權限
- 事件發生24小時內通報公路總局個資侵害事故，並發送Email通知可能受影響者
- 調整出租單功能並檢討資料安全管理措施，聯繫第三方檢測單位安排滲透測試、弱點掃描等檢測

圖片來源：格上GO Smart

格上 Go Smart 事件剖析

主要資安管理缺失

GCS設定不當

出租單連結為公開連結，可能透過技術取得非本人出租單

資料處理不當

未對機敏資料進行遮罩，導致用戶真實資料可能遭第三方瀏覽。

事件回應與影響

格上回應

- 第一時間清查該資料庫狀況無異常
- 加強相關資料庫安全並設置在國際認證的安全平台，根據ISO-27001資訊安全驗證
- 規範管理，定期進行掃描與高強度防火牆機制保護，確保資訊安全無虞。
- 針對可能受影響之客戶提供相關慰問措施。

事件影響

- 使用者之姓名、身分證、電話、地址、生日可能被第三人知悉
- 強化加密：個人出租單加上密碼功能
- 個資欄位顯示：遮罩出租單上個人資料
- 檔案不落地：出租單調整為客戶提出檢視需求時才產出，以封閉外部存取可能。

格上 Go Smart 事件交通部公路總局委外查核結果

援引法條		稽核發現
汽車運輸業個人資料檔案安全維護計畫及處理辦法	第四條第1項 業者就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。	經檢視格上汽車租賃股份有限公司「組織權責管理要點」並未包含個人資料管理專責組織。
	第三條第1項 保有消費者個人資料筆數達一百筆以上之業者，應依本辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫（以下簡稱本計畫），其內容應包含第四條至第二十二條規定之相關組織及程序，以落實個人資料檔案之安全維護與管理，防止被竊取、竄改、毀損、滅失或洩漏。	經查業者尚未訂定消費者個人資料檔案安全維護計畫，恐不利舉證消費者個資妥善維護管理，有礙健全經營之虞。

格上 Go Smart 事件交通部公路總局委外查核結果

援引法條		稽核發現
汽車運輸業個人資料檔案安全維護計畫及處理辦法	第十八條第1項 業者使用資通系統蒐集、處理或利用消費者個人資料達一百筆，且具對外電子商務服務系統者，應採取下列資料安全管理措施： 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、個人資料檔案及資料庫之存取控制與保護監控措施。 五、防止外部網路入侵對策。 六、非法或異常使用行為之監控與因應機制。	經查未發現對外電子商務服務系統執行「防止外部網路入侵對策」及「非法或異常使用行為之監控與因應機制」等情境之定期進行演練及檢討改善紀錄。

Go Smart 事件精進措施

事前

1. GCS權限設定委由專業第三方進行，確保設定正確
2. 個資相關服務查詢功能使用專屬連結，避免第三方取得
3. 遮蔽個資敏感資料，避免真實資料遭讀取
4. 設立個人資料管理專責組織
5. 依主管機關規定擬定相關個資安全維護計畫資料

事中

1. 立即發布聲明稿，向用戶說明事件緣由及防護措施
2. 確認有無其他系統存在風險
3. 依據相關辦法通報及進行危機處理

事後

1. 加強員工訓練，定期執行資安事件演練
2. 檢討資料安全管理措施，擴大與第三方資安廠商合作
3. 擬定完善諮詢管道及用戶補償措施，提醒用戶可能風險

iRent/格上Go Smart事件比較

	iRent	格上Go Smart
發生原因	暫存資料庫採用公開IP位置	出租單存放空間使用公開連結
發生日期	2023/1/28	2023/2/2
是否於知悉72小時內通報	否	是
影響會員數	142,509筆	約1.6萬筆
裁罰內容	依個人資料保護法第48條裁罰新台幣20萬元	尚無定案
用戶補償	受影響用戶發放汽車三小時優惠券一張+機車免起步價優惠券5張	受影響用戶補償300元時數卷

資通安全管理法及其子法簡介

資安法立法目的與規範對象

立法目的

- 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。

規範對象

公務機關 *不含軍事、情報機關

① 中央與地方機關(構)

② 公法人

特定非公務機關

① 關鍵基礎設施提供者

② 公營事業

③ 政府捐助之財團法人

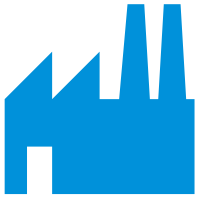
關鍵基礎設施提供者(CI)定義

- 指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關認定，並報主管機關核定者。

資安法規範適用先後

兼具公務機關及CI提供者

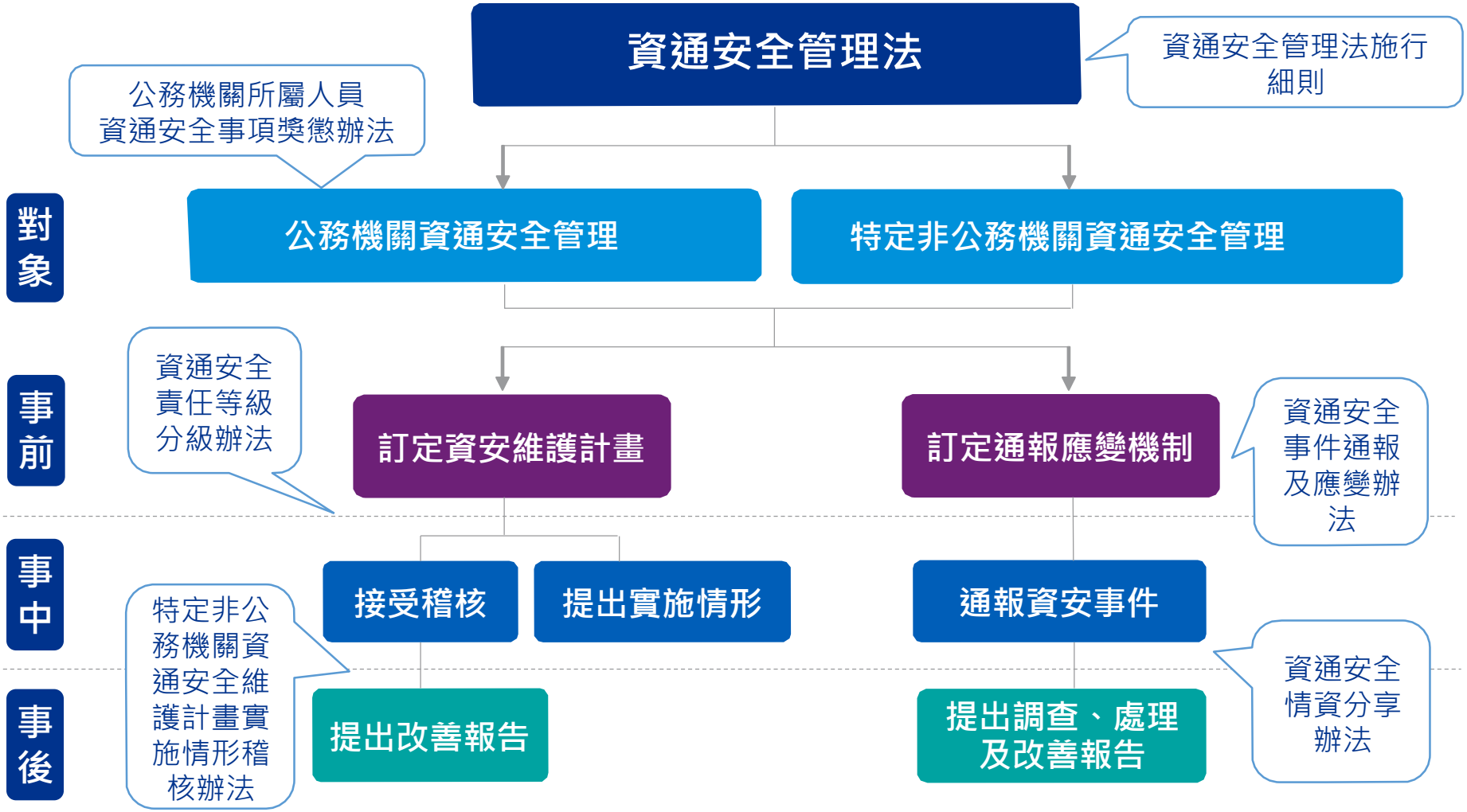
- 優先適用公務機關之規定
- 如：飛航服務總台



兼具公營事業/財團法人及CI提供者

- 優先適用CI提供者之規定
- 如：台電、中油

資通安全管理法架構


資通安全管理法
資通安全管理法施行細則
公務機關所屬人員資通安全事項獎懲辦法
對象
公務機關資通安全管理
特定非公務機關資通安全管理
事前
資通安全責任等級分級辦法
訂定資安維護計畫
訂定通報應變機制
資通安全事件通報及應變辦法
事中
接受稽核
提出實施情形
通報資安事件
特定非公務機關資通安全維護計畫實施情形稽核辦法
事後
提出改善報告
提出調查、處理及改善報告
資通安全情資分享辦法

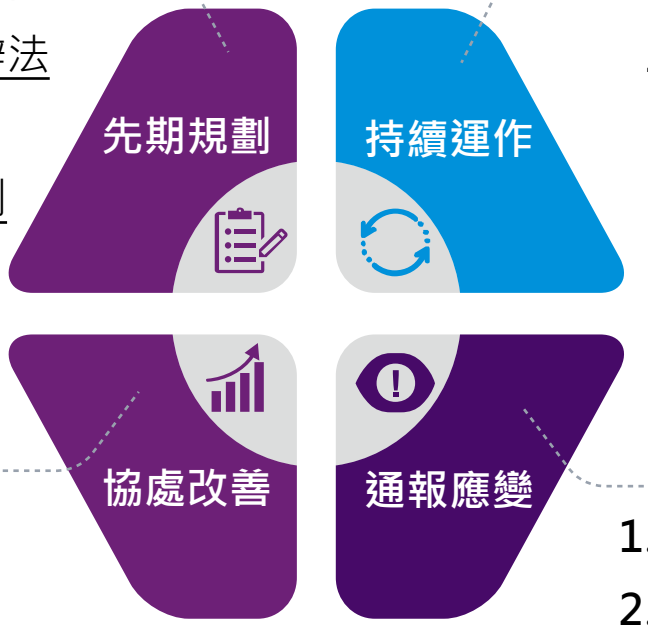
資通安全管理法子法架構

1. 機關資安責任等級分級提報

➢資通安全責任等級分級辦法

2. 訂定資安維護計劃

➢資通安全管理法施行細則



1. 提出資安維護計劃實施情形

2. 進行稽核

➢ 特定非公務機關資通安全維護計劃實施情形稽核辦法

1. 提出稽核改善報告

2. 情資分享

➢資通安全情資分享辦法

3. 人員獎懲

➢公務機關所屬人員資通安全事項獎懲辦法

1. 訂定資安事件通報應變機制

2. 通報資安事件

3. 提出事件調查改善報告

➢資通安全事件通報及應變辦法

資安法規範內容五大重點

主管機關(行政院)應辦事項

- 行政院、委託或委任單位、各公務機關
- 中央目的事業主管機關權責
- 權限委託

立法目的與名詞定義

- 資安責任等級分級
- 資安維護計畫之制定與 實施
- 年度資安維護計畫 實施情形提出
- 資安稽核
- 資安事件通報應變
- 改善報告
- 公告
- 定期公布國家資通安全情勢報告及資通安全發展方案
- 建立情資分享機制

罰則

- 公務機關人員獎懲標準
- 通報義務
- 資安維護計畫實施
- 改善報告
- 應變機制

公務機關資通安全管理

- 資安責任等級分級
- 資安維護計畫之制定與實施
- 資安長設置
- 年度資安維護計畫實施情形提出
- 資安稽核
- 改善報告
- 資安事件通報應變
- 公務機關人員獎懲標準

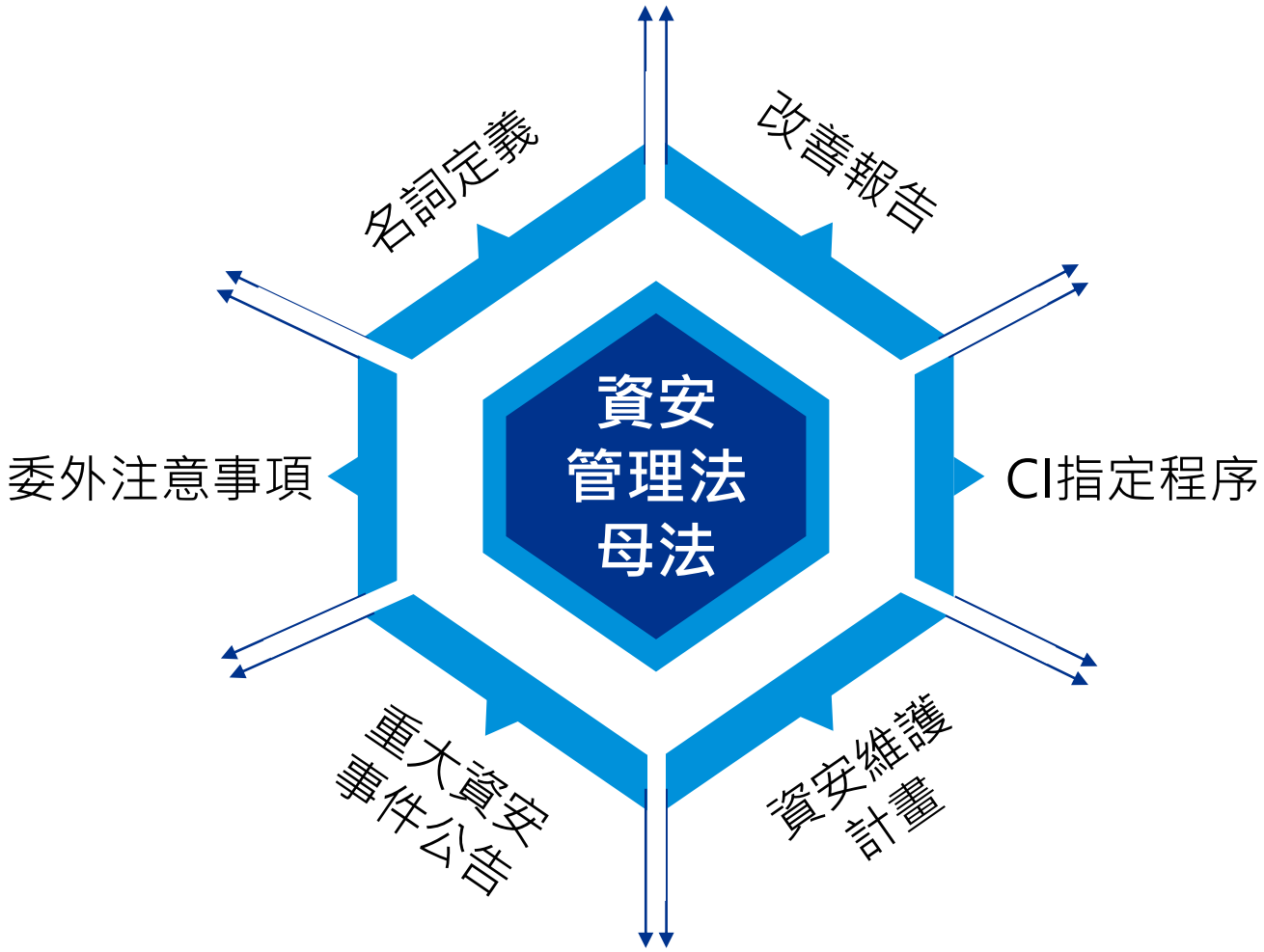
特定非公務機關資通安全管理

- 資安責任等級分級
- 資安維護計畫之制定與實施
- 年度資安維護計畫實施情形提出
- 資安稽核
- 資安事件通報應變
- 改善報告
- 重大資安事件公告
- 罰則

資通安全管理法各章節摘要

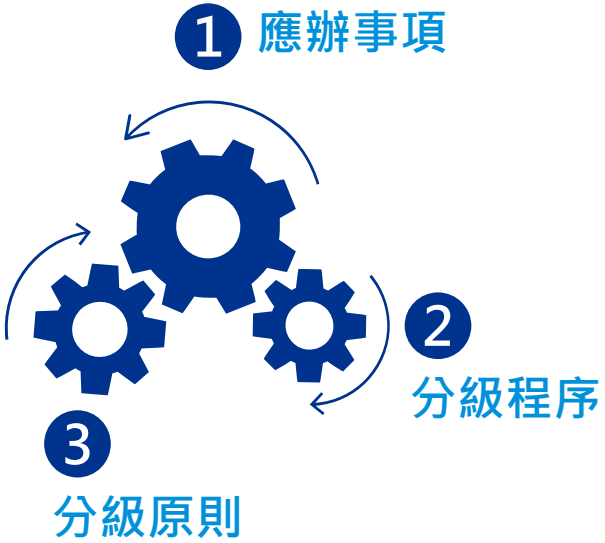
第一章 總則(1-9)	立法目的、名詞解釋、資通安全產業之推動、行政院職責、事務委任或委託、資安責任等級分級、情資分享機制、資通委外監督。
第二章 公務機關資通安全管理(10-15)	資通安全管理與維護計畫、資通安全長之設置、年度資通安全維護計劃實施情形、通報應變措施、獎懲措施。
第三章 特定非公務機關資通安全管理(16-18)	關鍵基礎設施及其他特定非公務機關之資通安全責任等級、資通安全維護計劃實施情形、主管機關稽核、限期改善。
第四章 罰則(19-21)	行政處分。
第五章 附則(22-23)	施行細則、施行日期，由主管機關訂之。

資通安全管理法施行細則架構



資通安全責任等級分級辦法

> 機關應考量其業務、資訊、系統、機關層級等因素訂定機關資安責任等級。

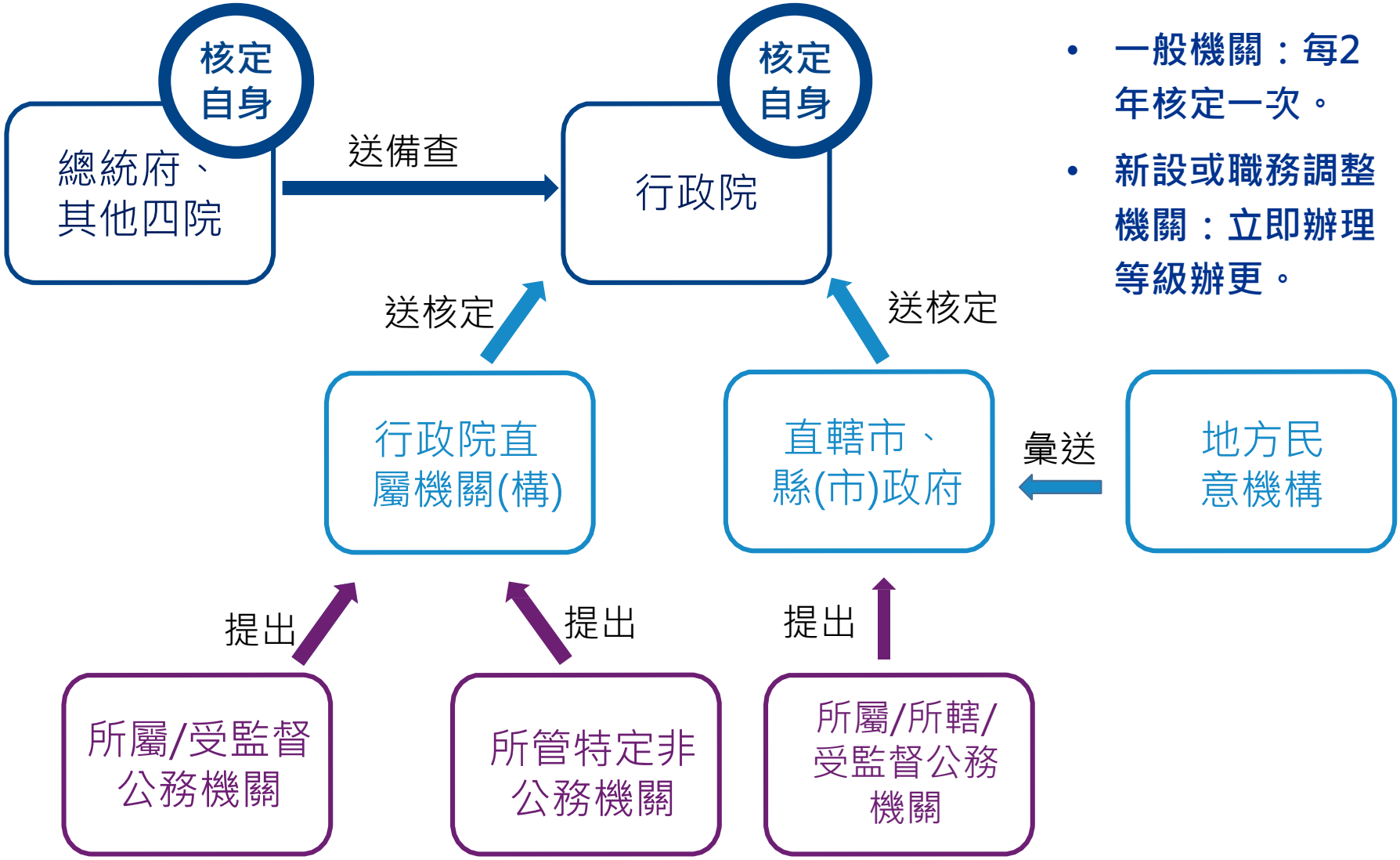


考慮因素

資通安全責任等級分級原則

§10：各機關得考慮其對國家 安全、社會公益或人民之影響， 彈性調整其等級

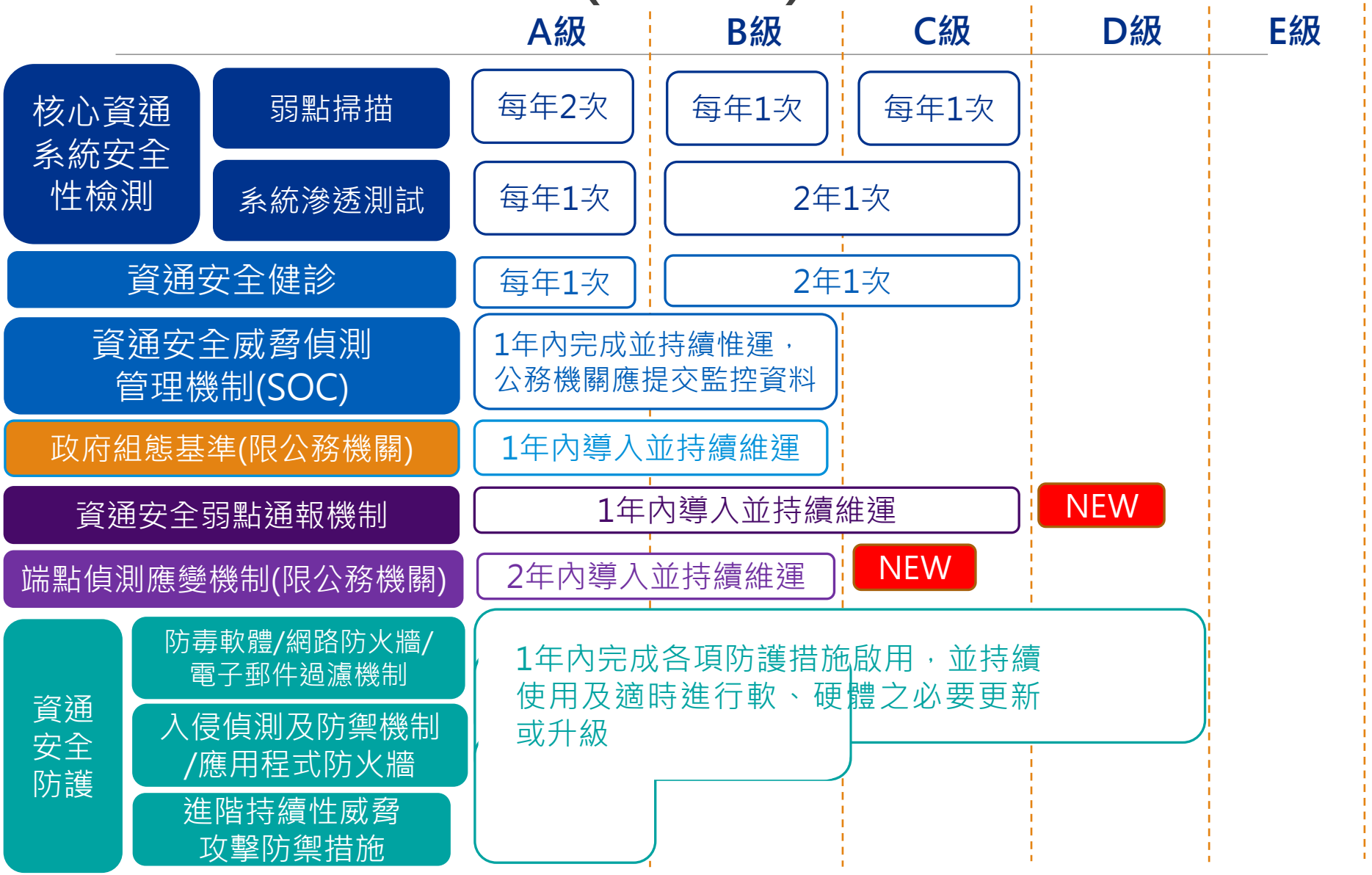
資通安全責任等級分級程序



- **一般機關：每2年核定一次。**
- **新設或職務調整機關：立即辦理等級辦更。**

各責任等級應辦事項(管理面)

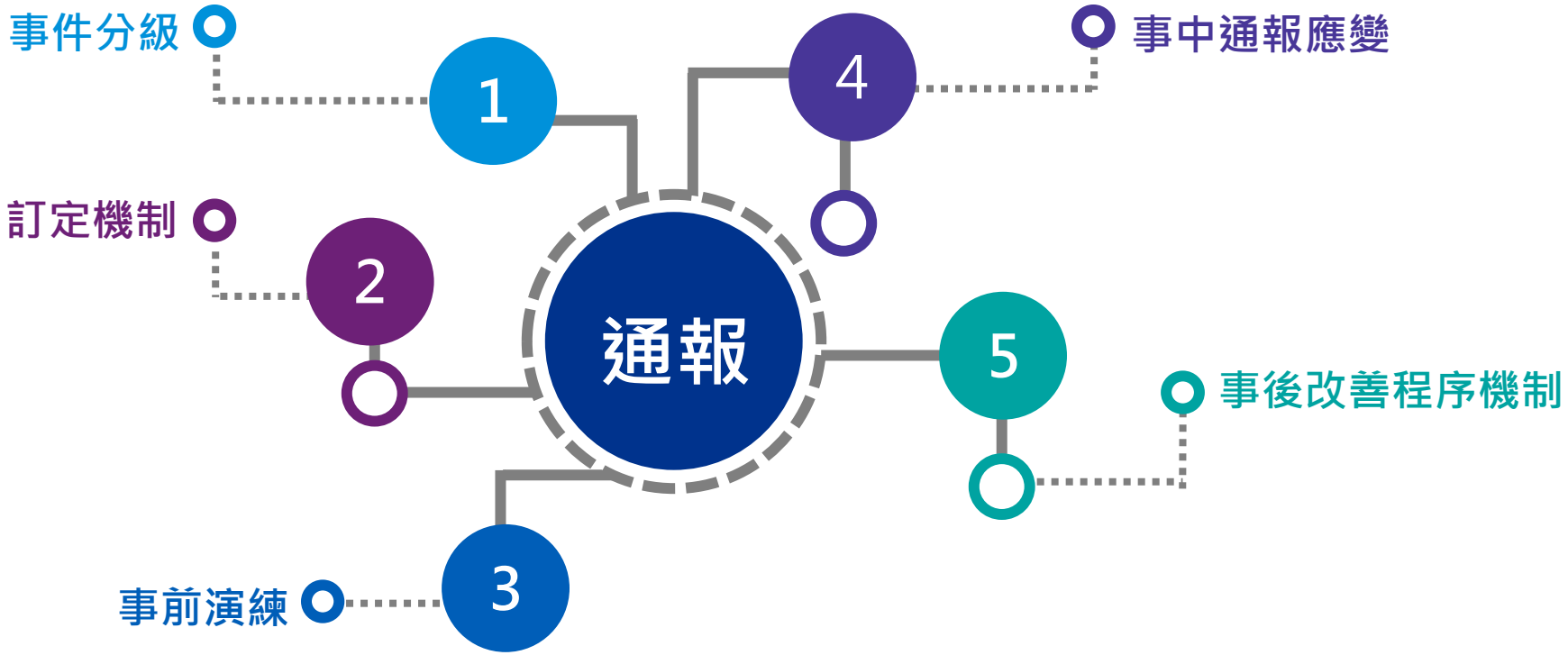
各責任等級應辦事項(技術面)



各責任等級應辦事項(認知與訓練面)

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



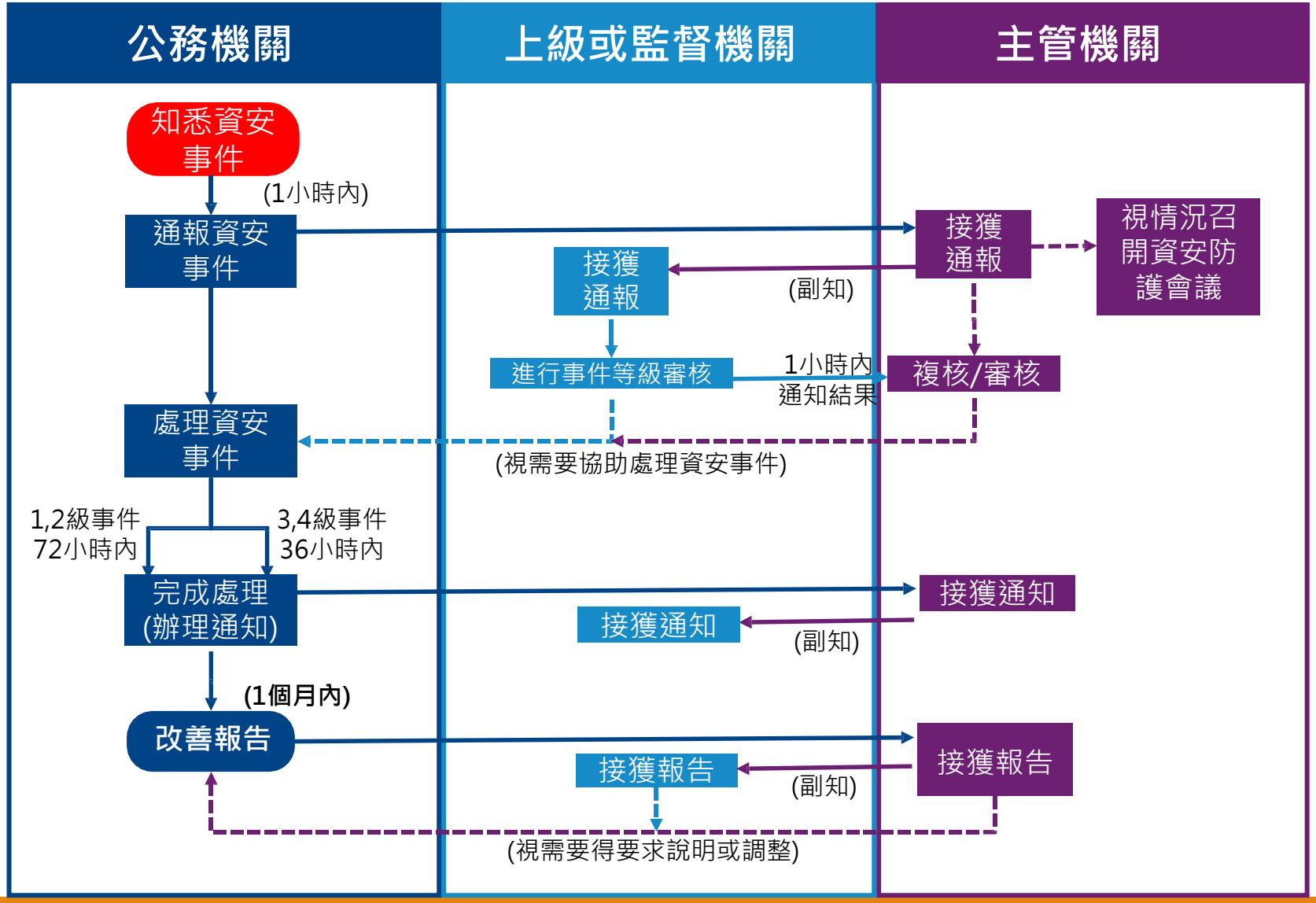
資通安全事件等級分類

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，造成機關日常作業影響。
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，於可容忍中斷時間內回復正常運作。

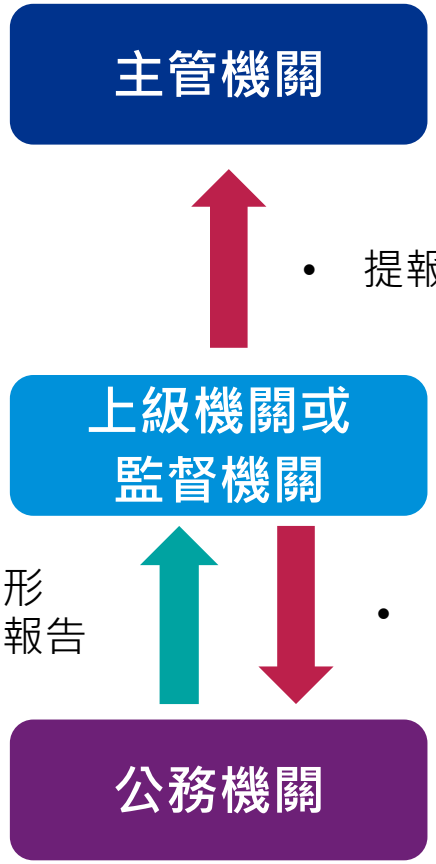
資通安全事件等級分類(續)

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、敏感資訊或涉及關鍵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。
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。

事件通報流程-公務機關


公務機關
上級或監督機關
主管機關
知悉資安事件
(1小時內)
通報資安事件
接獲通報
(副知)
接獲通報
視情況召開資安防護會議
進行事件等級審核
1小時內通知結果
複核/審核
處理資安事件
(視需要協助處理資安事件)
1,2級事件72小時內
3,4級事件36小時內
完成處理(辦理通知)
接獲通知
接獲通知
(副知)
(1個月內)
改善報告
接獲報告
接獲報告
(副知)
(視需要得要求說明或調整)

角色與權責-公務機關

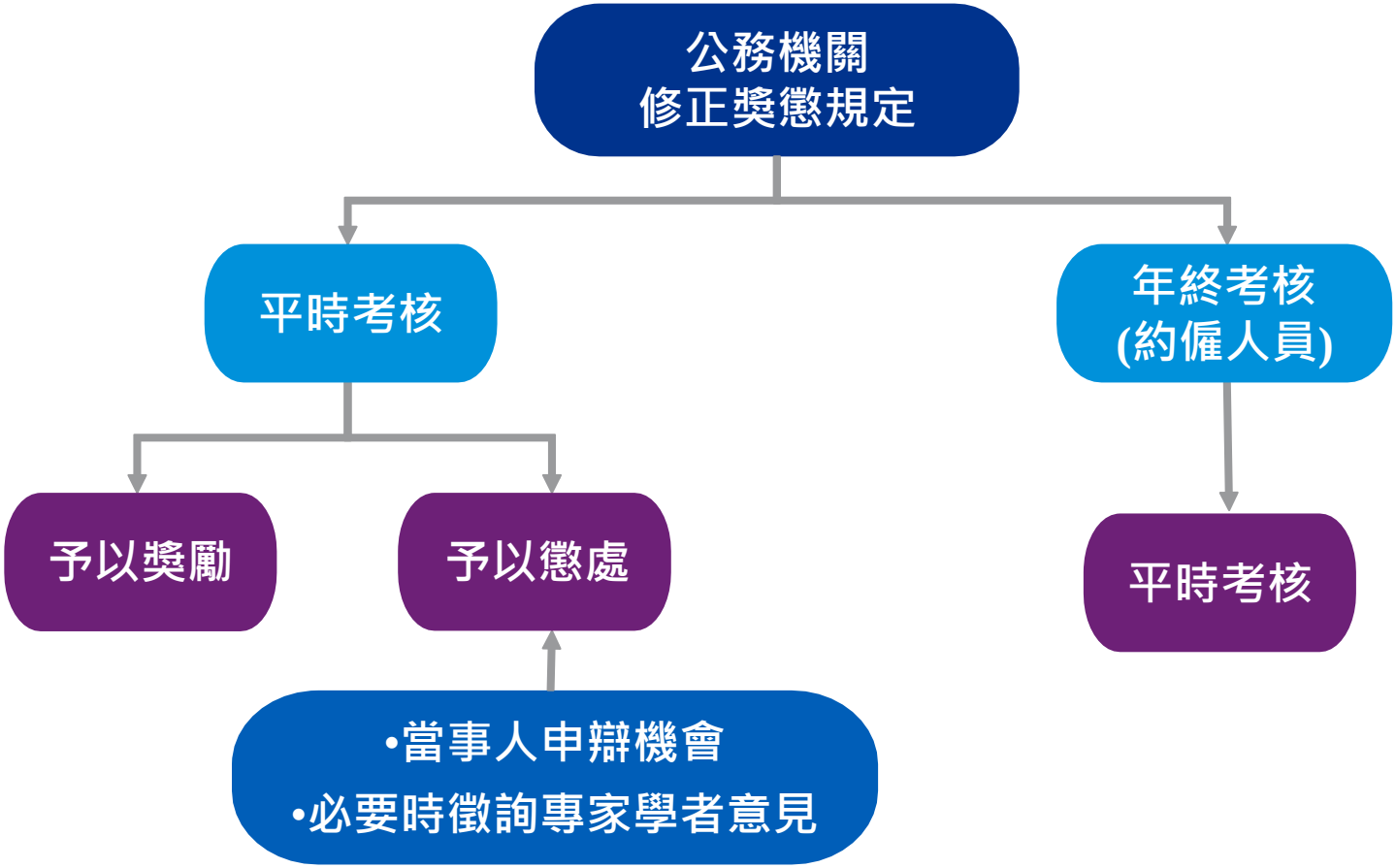


- 提報自身及所屬資安責任等級
- 提報資安維護計畫實施情形
- 通報資安事件及提出改善報告
- 進行資安稽核

- 設置資安長
- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

公務機關所屬人員資通安全事項獎懲辦法

- 敦促公務機關所屬人員執行資通安全維護事務。



公務機關所屬人員資通安全事項獎懲辦法(續)

依資通安全管理法第十五條第二項及第十九條第二項規定訂定

第三條 有下列情形之一者，予以獎勵：

一、依本法、本法授權訂定之法規或機關內部規範，訂定、修正及實施資通安全維護計畫，績效優良。

二、稽核所屬或監督機關之資通安全維護計畫實施情形，或辦理資通安全演練作業，績效優良。

三、配合主管機關、上級或監督機關辦理資通安全維護計畫實施情形之稽核或資通安全演練作業，經評定績效優良。

四、辦理資通安全業務切合機宜，防止資通安全事件之發生，避免本機關、其他機關或人民遭受損害。

五、主動發現新型態之資通安全弱點或入侵威脅，並進行資通安全情資分享，防止資通安全事件之發生或降低其損害。

六、積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。

七、對資通安全業務提出具體建議或革新方案，並經採行。

八、辦理資通安全人才培育事務，有具體貢獻。

九、辦理資通安全科技之研發、整合、應用、產學合作或產業發展事務，有具體貢獻。

十、辦理資通安全軟硬體技術規範、相關服務及審驗機制發展等事務，有具體貢獻。

十一、辦理資通安全政策、法制研析或國際合作事務，有具體貢獻。

十二、辦理其他資通安全業務有具體功績。

公務機關所屬人員資通安全事項獎懲辦法(續)

依資通安全管理法第十五條第二項及第十九條第二項規定訂定

第四條 有下列情形之一者，予以懲處：

一、未依本法、本法授權訂定之法規或機關內部規範辦理下列事項，情節重大：

（一）資通安全情資分享作業。

（二）訂定、修正及實施資通安全維護計畫。

（三）提出資通安全維護計畫實施情形。

（四）辦理資通安全維護計畫實施情形之稽核。

（五）配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。

（六）訂定資通安全事件通報及應變機制。

（七）資通安全事件之通報或應變作業。

（八）提出資通安全事件調查、處理及改善報告。

二、辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。

三、其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

四、對業務督導不力，致其屬員、所屬或所監督機關之人員有前三款情形之一。

資通安全維護計畫實施情形填報注意事項

資通安全維護計畫實施情形填報注意事項

- 須依格式填寫辦理情形。
- 考參考範本描述方式填寫。

資安維護計畫實施情形填寫範例(1/7)

實施項目	實施內容	實施情形說明
1.核心業務及其重要性	1.1資通業務及重要性盤點	本校資通業務及重要性詳參資通安全維護計畫（詳附件）。
2.資通安全政策及目標之訂定	2.1資通安全政策訂定及核定	本校已訂定資通安全政策，詳參資通安全維護計畫，並經校長核定（詳附件）。
	2.2資通安全目標之訂定	本校已訂定資通安全目標，詳資通安全維護計畫。
	2.3資通安全政策及目標宣導	本校為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4資通安全政策及目標定期檢視	本校已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性（詳會議記錄）。

資安維護計畫實施情形填寫範例(2/7)

實施項目	實施內容	實施情形說明
3.設置資通安全推動組織	3.1設定資通安全長	本校已指定OOO校長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2設置資通安全推動小組	本校已設置資通安全推動小組，其組織、分工及職掌詳參資通安全維護計畫。
4.專責人力及經費之配置	4.1專職(責)人員配置	本校依規定配置資通安全人員1名。
	4.2經費之配置	本校本學年度資安經費佔資訊經費之○○%。

資安維護計畫實施情形填寫範例(3/7)

實施項目	實施內容	實施情形說明
5.資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1資訊及資通系統之盤點	本校已於○年○月盤點資訊、資通系統，建立資產目錄
	5.2機關資通安全責任等級分級	本校依資通安全責任等級分級辦法，為資通安全責任等級D級機關。
6.資通安全風險評估	6.1資通安全風險評估	本校已於○年○月完成資訊、資通系統及相關資產之風險分析評估及處理。
	6.2資通安全風險之因應	本校已依資通安全風險評估之結果，擬定對應資通安全防護及控制措施。

資安維護計畫實施情形填寫範例(4/7)

實施項目	實施內容	實施情形說明
7.資通安全防護及控制措施	7.1資訊及資通系統之保管	本校已依安全維護計畫辦理，詳附件資料。
	7.2存取控制與加密機制管理	本校已依資通安全維護計畫辦理。
	7.3作業及通訊安全管理	本校已依資通安全維護計畫辦理。
	7.4資通安全防護設備	本校已依資通安全維護計畫辦理。

資安維護計畫實施情形填寫範例(5/7)

實施項目	實施內容	實施情形說明
8.資通安全事件通報、應變及演練相關機制	8.1訂定資通安全事件通報、應變及演練相關機制	本校已依教育機構資安通報平台規定辦理。
	8.2資通安全事件通報、應變及演練	本校已依教育機構資安通報平台規定進行資通安全事件通報；並已於學年初配合辦理通報應變演練。
9.資通安全情資之評估及因應機制	9.1資通安全情資之分類評估	本校接受局端情資後，配合辦理。
	9.2資通安全情資之因應措施	本校已接受局端情資之分類，採取對應之因應措施。

資安維護計畫實施情形填寫範例(6/7)

實施項目	實施內容	實施情形說明
10.資通系統或服務委外辦理之管理	10.1選任受託者應注意事項	本校資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2監督受託者資通安全維護情形應注意事項	本校已依規定監督受託者資通安全維護情形。
11.資通安全教育訓練	11.1資通安全教育訓練要求	已要求本校人員完成資通安全通識教育訓練三小時，教職員人數共O人，O人完成教育訓練取得時數。
	11.2辦理資通安全教育訓練	本校已於學年初結合新進教師研習，辦理資通安全教育訓練。
12.公務機關所屬人員辦理業務涉及資通安全事項之考核機制	1. 訂定考核機制並進行考核	本校已建立考核機制，並已依規定進行平時及年終考核。

資安維護計畫實施情形填寫範例(7/7)

實施項目	實施內容	實施情形說明
13.資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1資通安全維護計畫之實施	本校已依資通安全維護計畫規定，據以實施並保存相關之執行成果記錄。
	13.2資通安全維護計畫實施情形之稽核機制	本校已依規定辦理內部自我檢核。
	13.3資通安全維護計畫之持續精進及績效管理	本校已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

問題與討論