新北市政府教育局

資安訪視常見議題

講師：葉益禎

中華民國113年8月13日

課程大綱

序號	大綱
一	如何符合資通安全管理法之要求
二	資通安全管理法修法重點說明
三	校園資安訪視常見議題
四	如何做好校園資通安全管理
五	問題與討論

如何符合資通安全管理法之要求

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

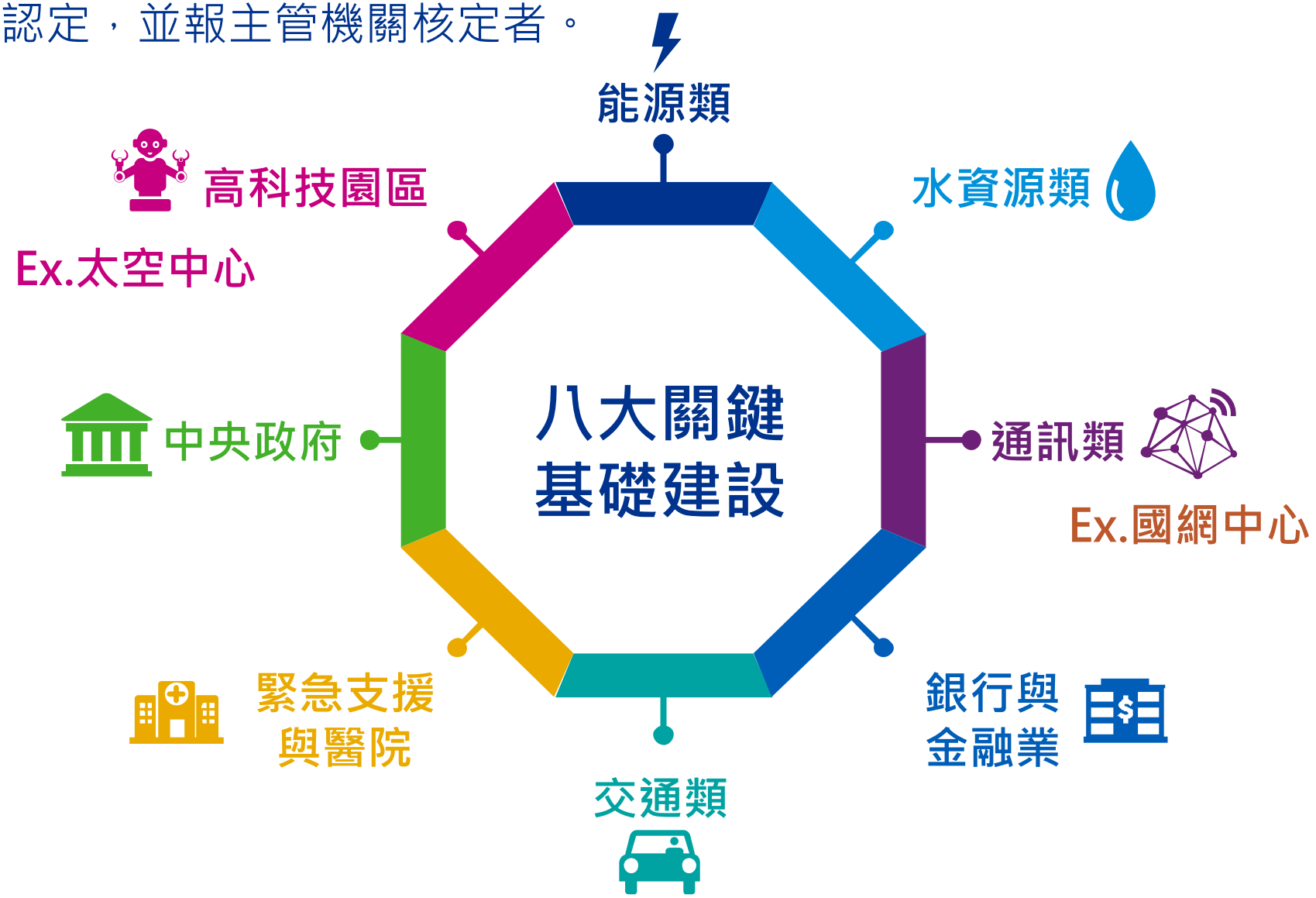
① 關鍵基礎設施提供者

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

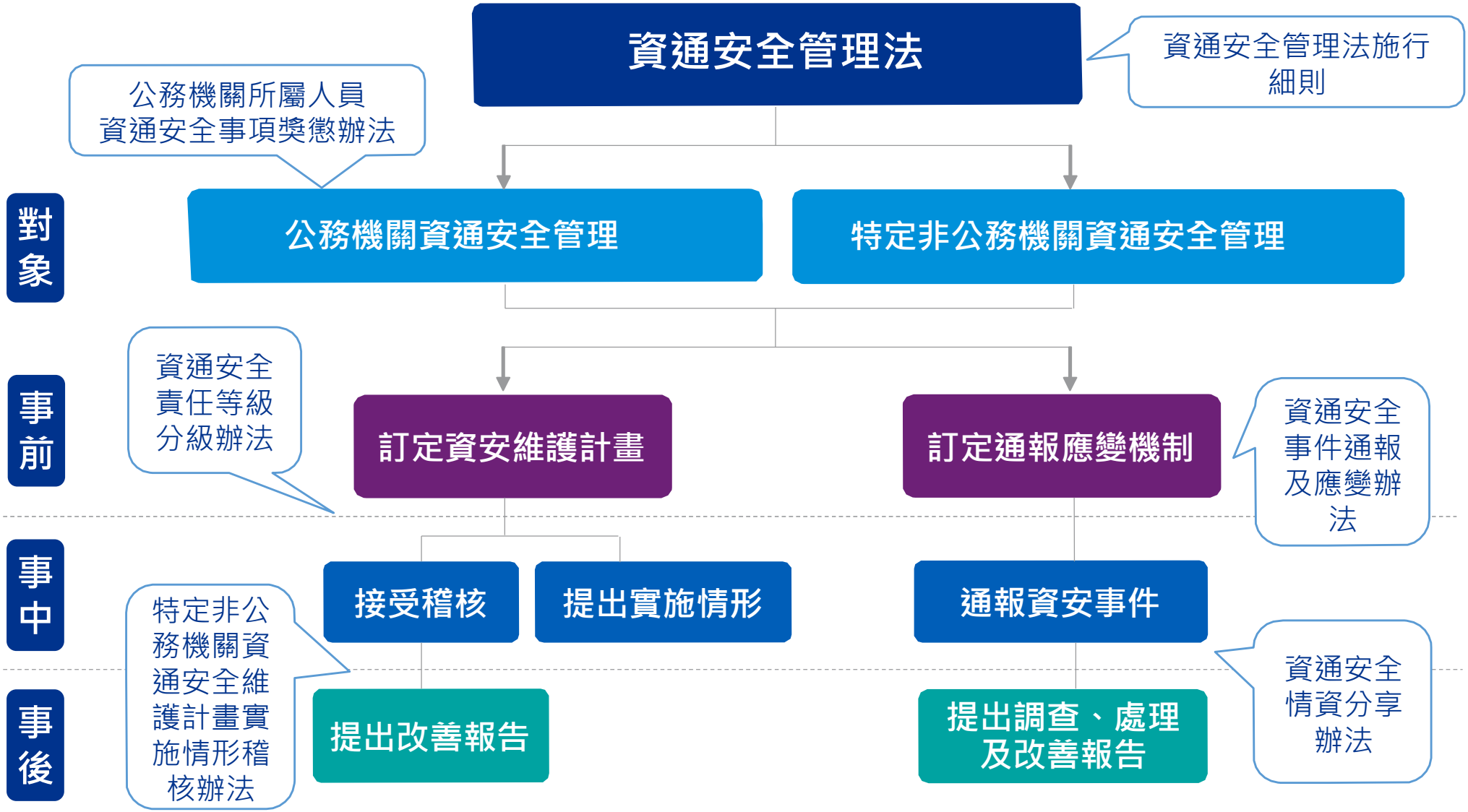
兼具公務機關及CI提供者

- 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

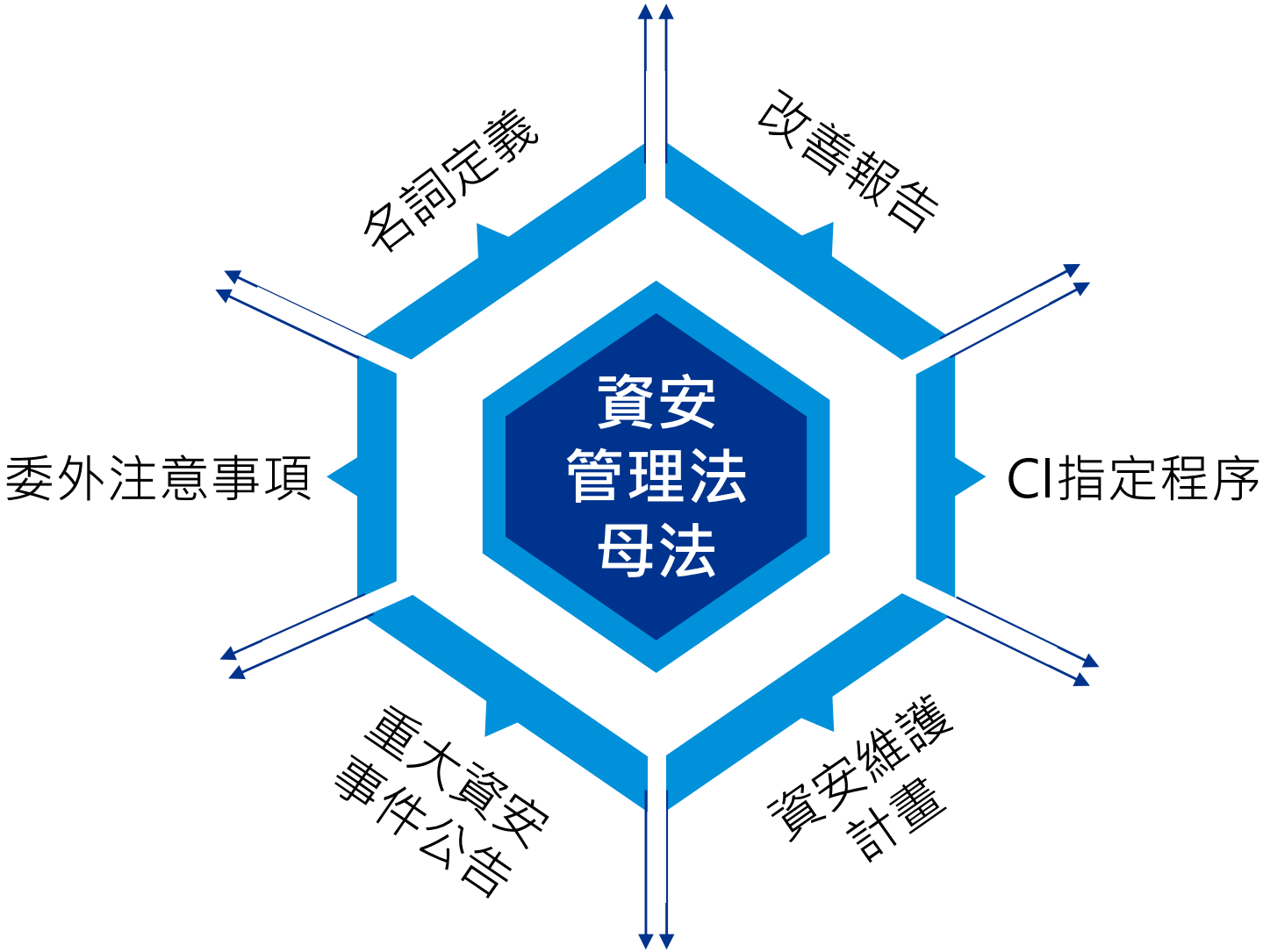
特定非公務機關資通安全管理

- 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重點摘要

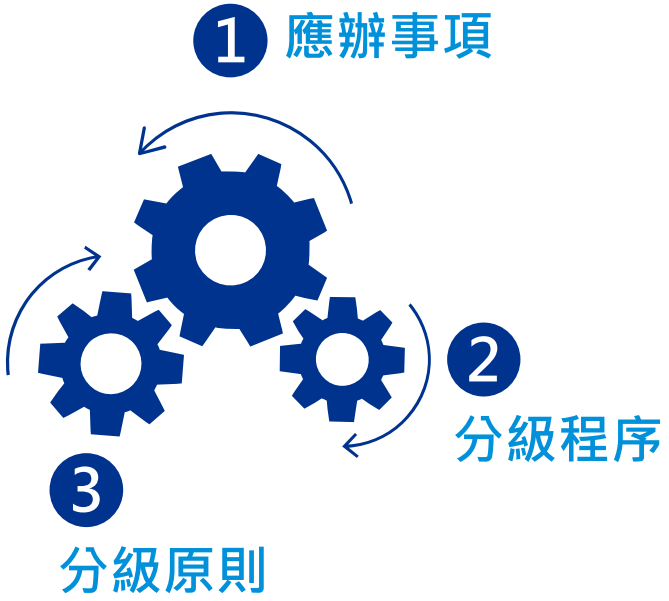
第一章 總則(1-9)	立法目的、名詞解釋、資通安全產業之推動、行政院職責、事務委任或委託、資安責任等級分級、情資分享機制、資通委外監督。
第二章 公務機關資通安全管理(10-15)	資通安全管理與維護計畫、資通安全長之設置、年度資通安全維護計劃實施情形、通報應變措施、獎懲措施。
第三章 特定非公務機關資通安全管理(16-18)	關鍵基礎設施及其他特定非公務機關之資通安全責任等級、資通安全維護計劃實施情形、主管機關稽核、限期改善。
第四章 罰則(19-21)	行政處分。
第五章 附則(22-23)	施行細則、施行日期，由主管機關訂之。

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。

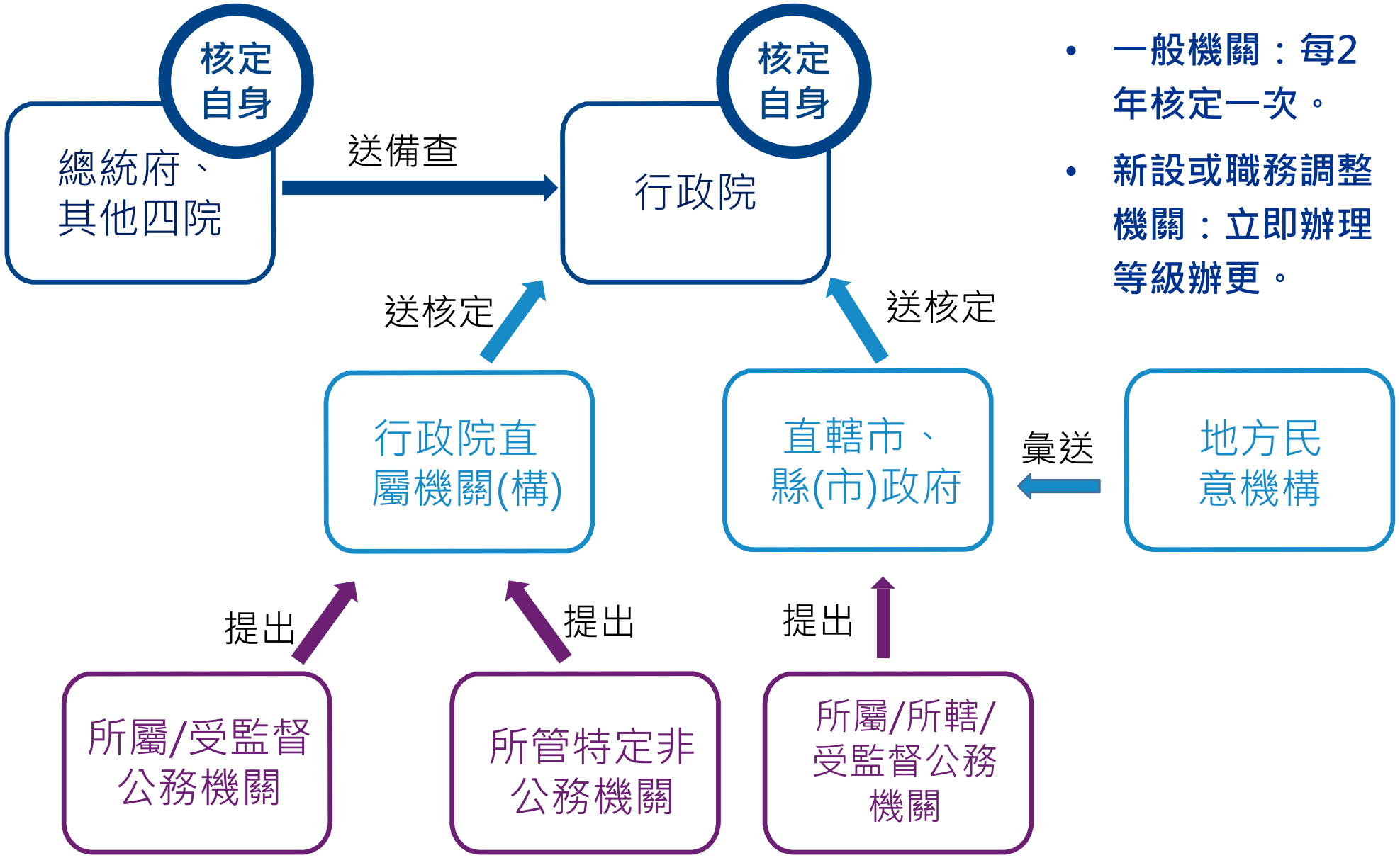


資通安全責任等級分級原則

- **A級**：全國性
- **B級**：區域或地區性或研發國家核心科技
- **C級**：有自行或委外開發資通系統，並設置伺服器者
  (具權限區分及管理功能)
- **D級**：未自行或委外開發資通系統，未設置伺服器
- **E級**：全部資通業務由其他機關兼辦或代辦

§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

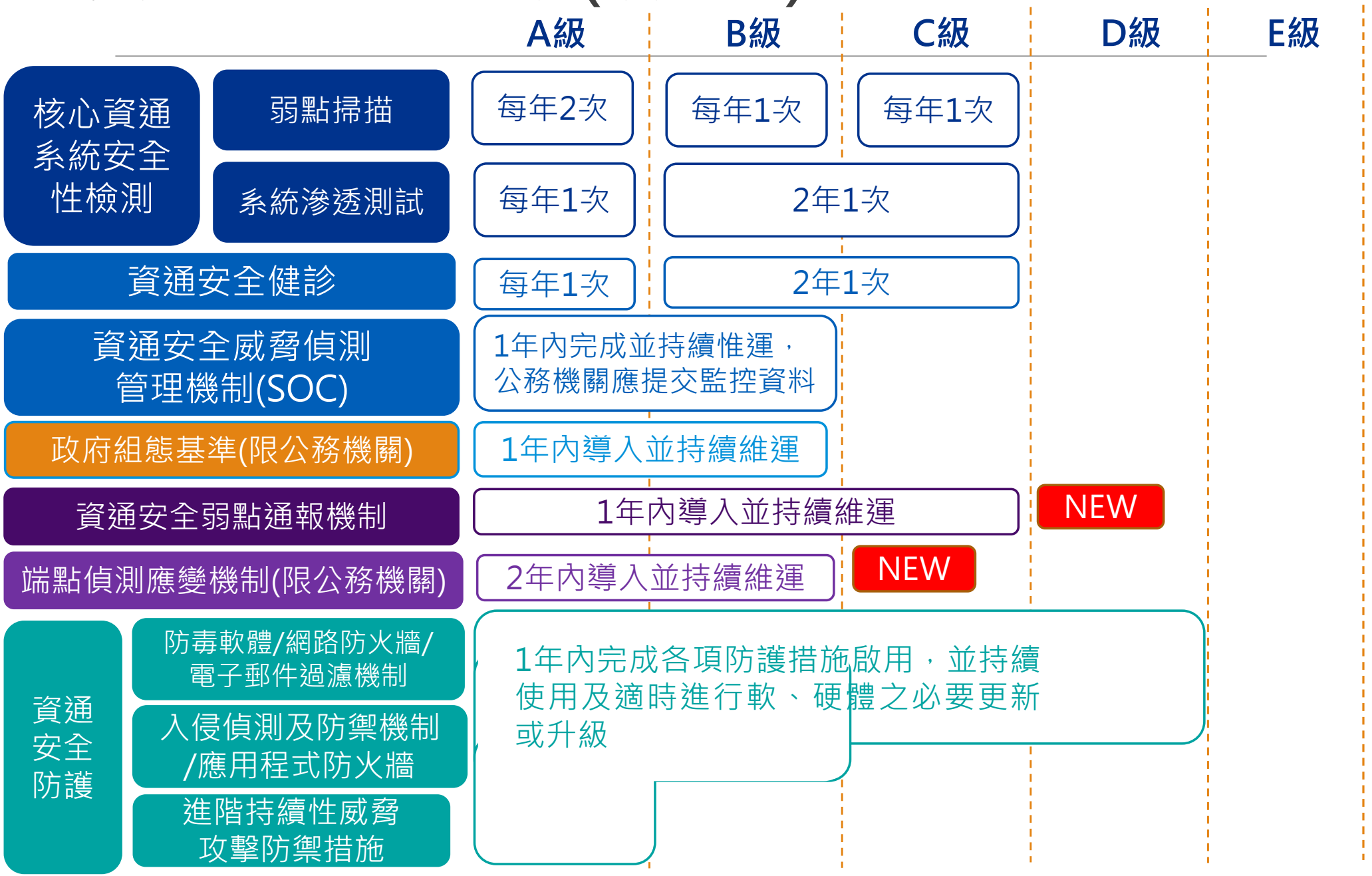
資通安全責任等級分級程序



- **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)

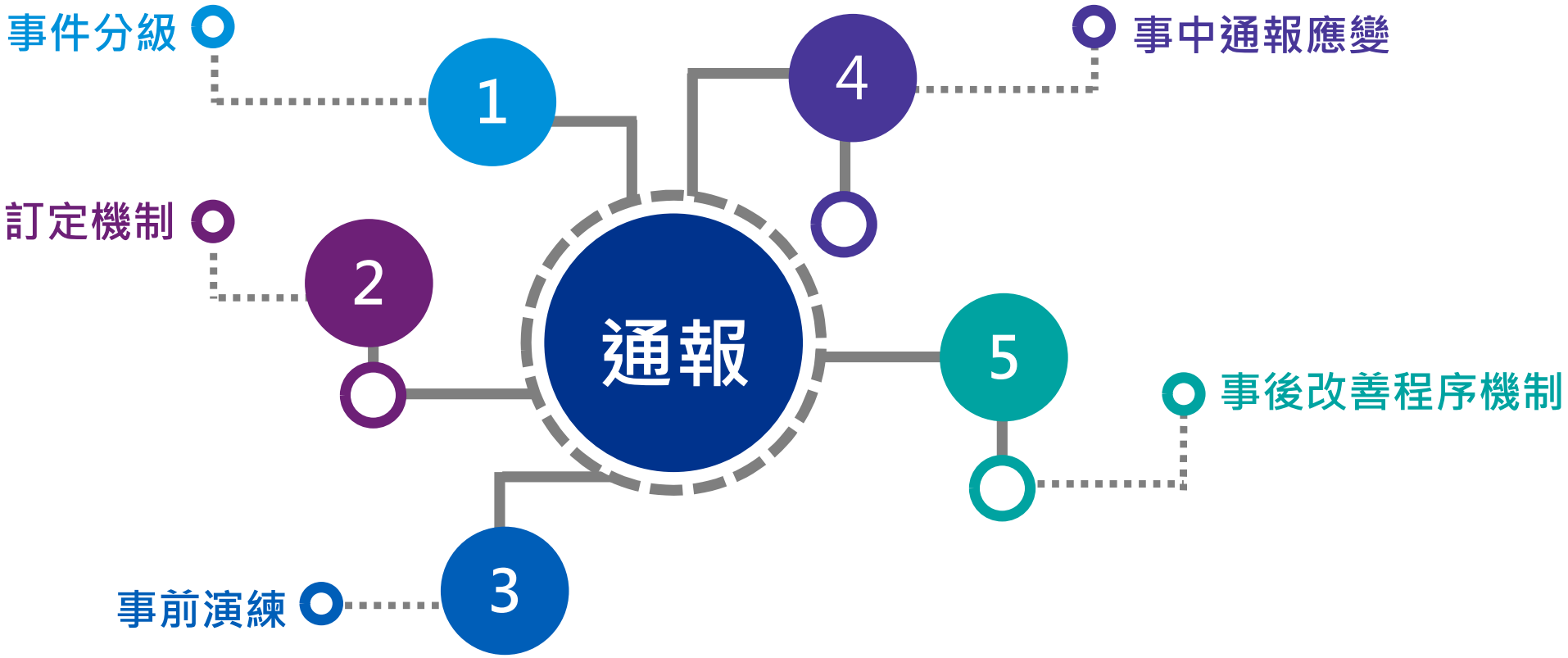
各責任等級應辦事項(技術面)



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。

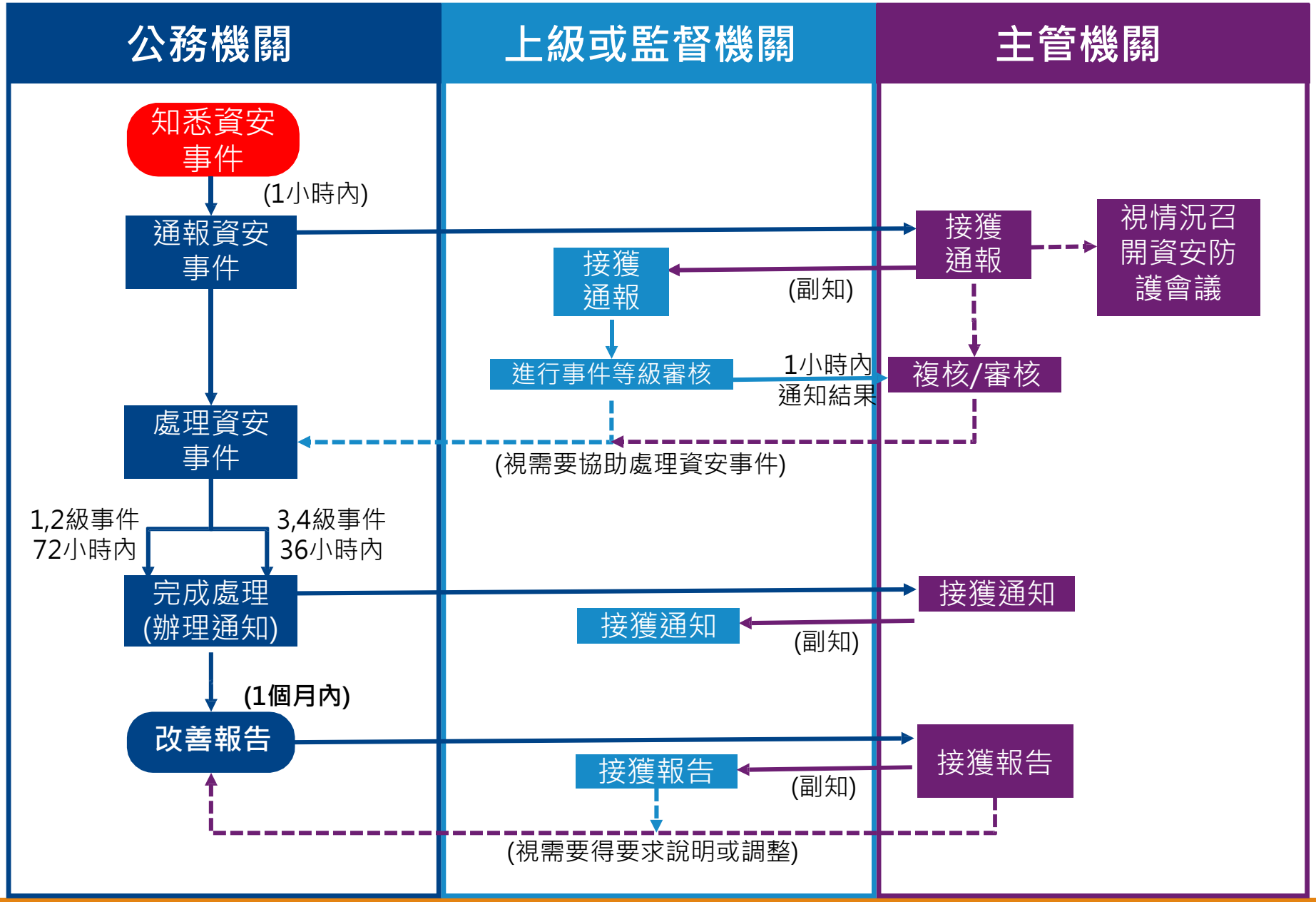
資通安全事件等級分類(續)

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。

資安事件等級判定

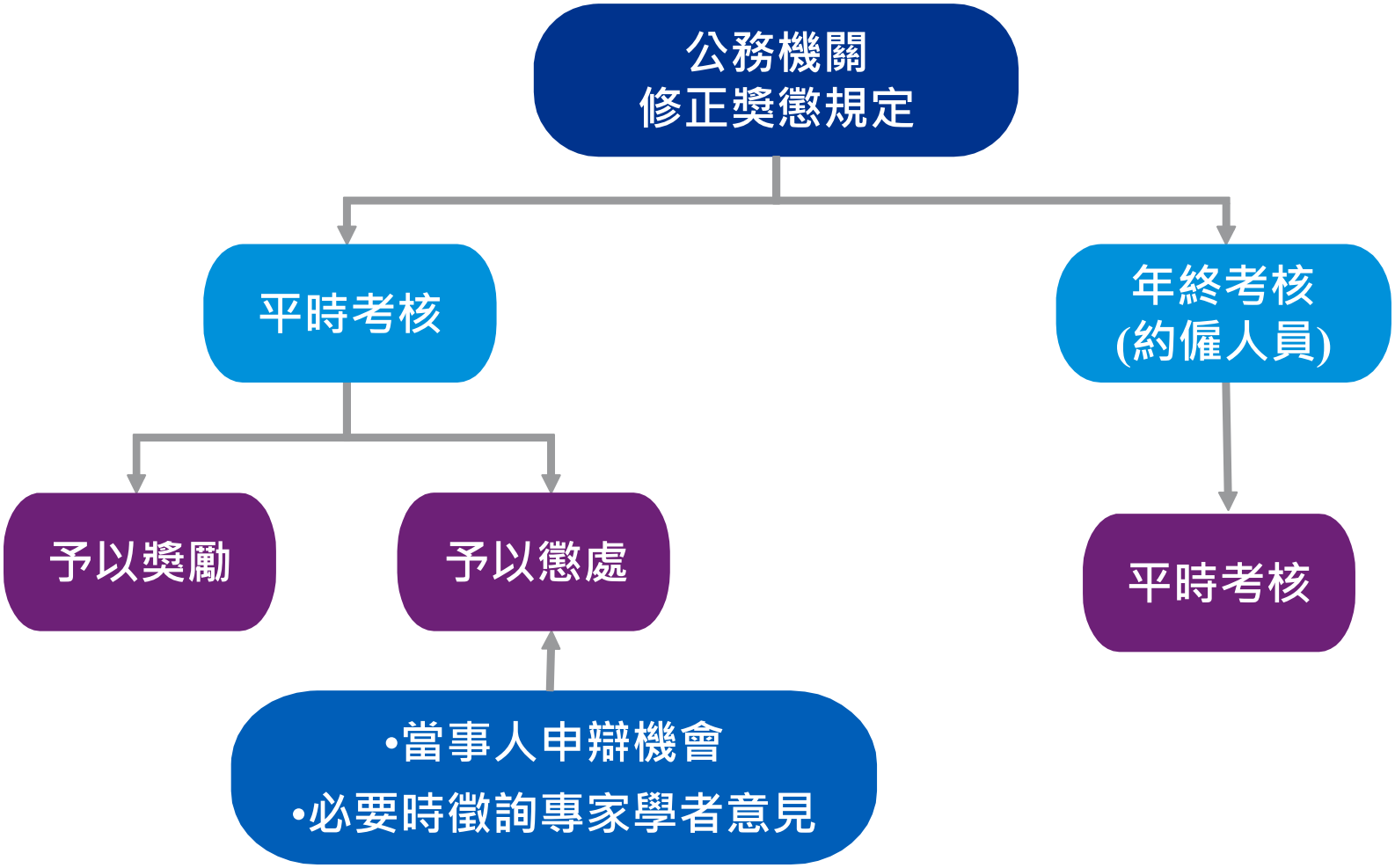
面向	程度	非核心業務	核心業務		敏感資訊、公務機密
			非關鍵基礎設施	關鍵基礎設施	國家機密(4級)
機密性 Confidentiality	輕微洩漏	1級	2級	3級	3級
	嚴重洩漏	2級	3級	4級	4級
完整性 Integrity	輕微竄改	1級	2級	3級	3級
	嚴重竄改	2級	3級	4級	4級
可用性 Availability	**可**於可容忍中斷時間回復	1級	2級	3級	NA
	無法於可容忍中斷時間回復	2級	3級	4級	NA

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
接獲通報
(副知)
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)

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。

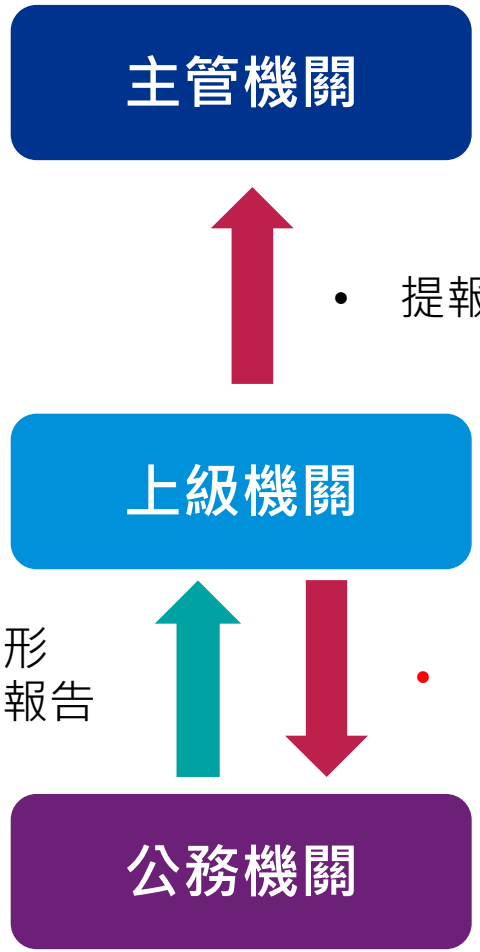
（八）提出資通安全事件調查、處理及改善報告。

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。

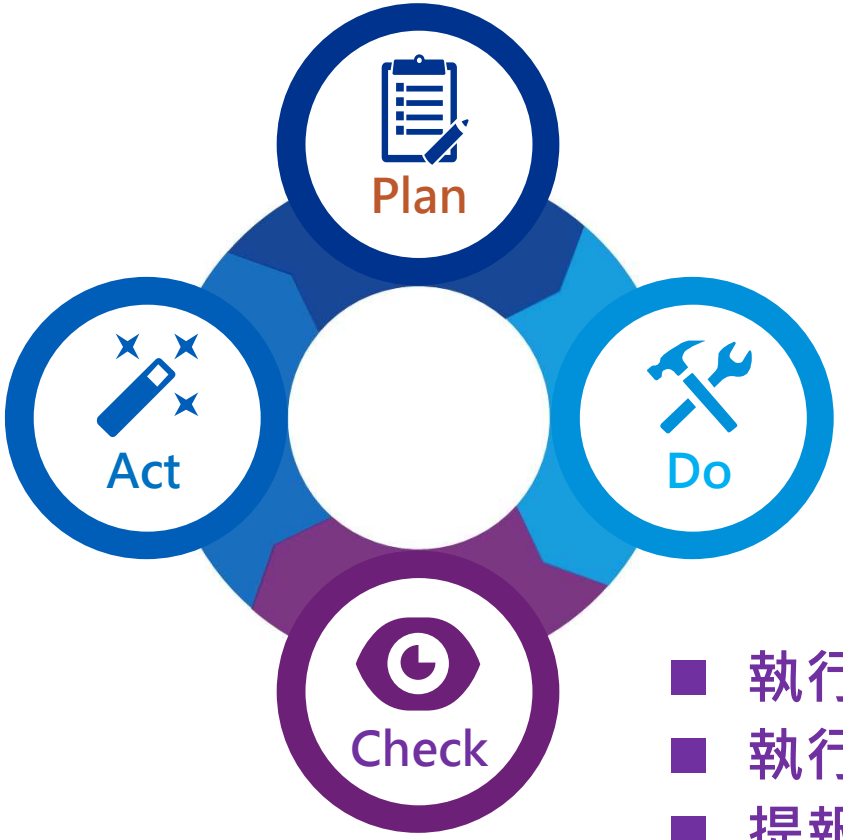
角色與權責-公務機關



- 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

資通安全管理法落實方式

- 訂定資安維護計畫
- 執行資訊資產盤點作業
- 執行風險評鑑與處理作業
- 執行資通系統分級與防護基準評估



- 執行改善措施

- 執行「資安責任等級分級辦法」之各項應辦事項
- 執行資通安全防護及控制措施
- 執行資安事件通報與應變機制

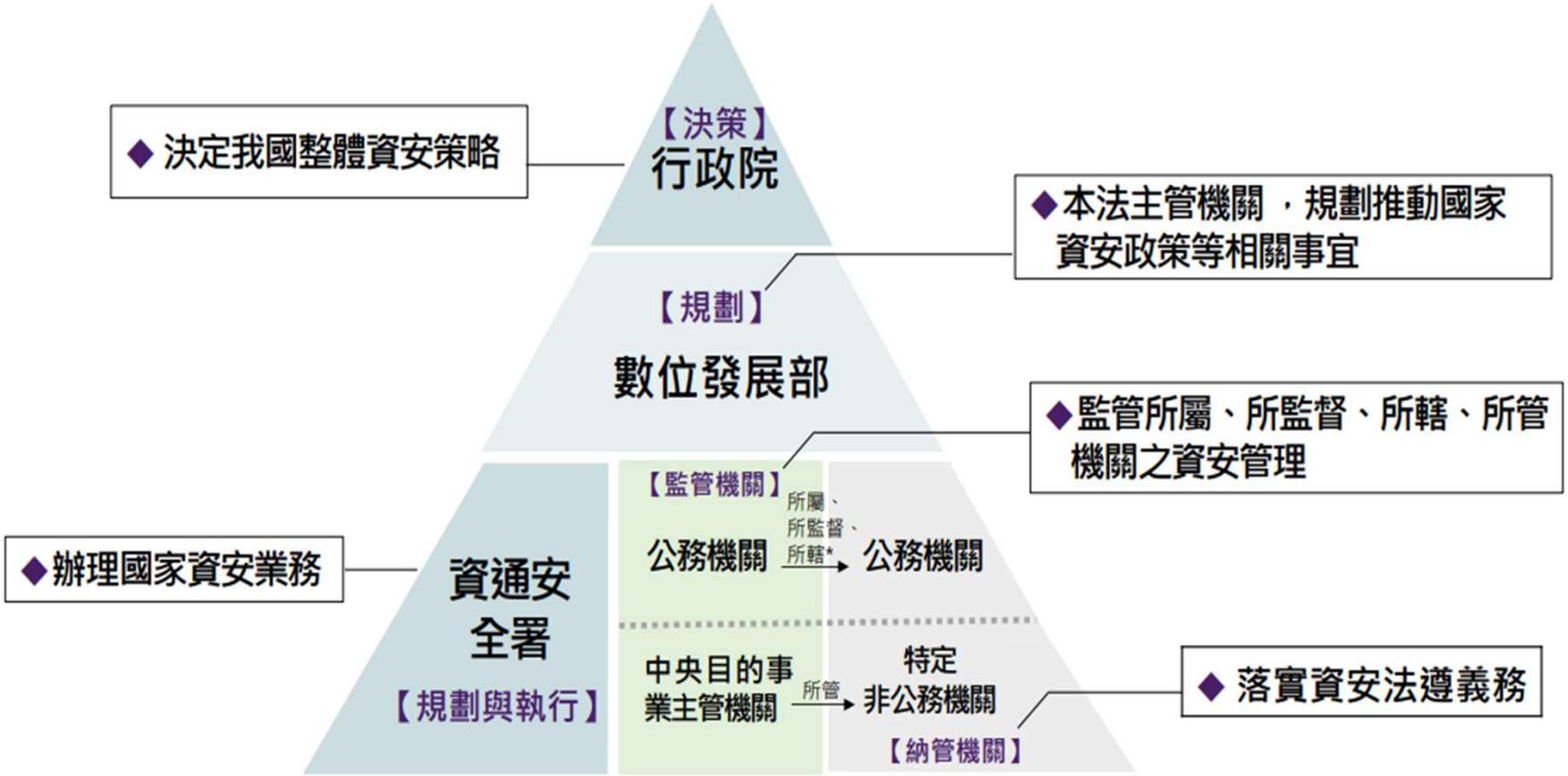
- 執行資通安全內部稽核作業
- 執行委外廠商稽核或監督
- 提報資安維護計畫實施情形

26

資通安全管理法修法重點說明

資安法修訂-重點1明確機關權責強化合作協力

■明定本法主管機關及各機關權責



所轄公務機關：在直轄市政府係指直轄市山地原住民區公所及直轄市山地原住民區民代表會；在縣政府係指鄉（鎮、市）公所、鄉（鎮、市）民代表會

圖片來源: 資安署-資通安全管理法修法簡報

資安法修訂-重點2強化納管機關資安管理

■(1)共通規範:危害國家資通安全產品相關規範

NEW
新增條文

公務機關

限制範圍

- 機關本身
- 場所：提供公眾視聽或使用之傳播設備及網際網路接取服務
- 公務人員獲配之公務用資通訊設備(*不適用下方限制方式之但書)

限制方式

- 原則：不得下載、安裝或使用
- 但書：因業務需求且無其他替代方案者，專案使用

特定非公務機關

限制範圍

- 特定非公務機關本身
- 場所：提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時

限制方式

- 原則：中央目的事業主管機關，得予以限制或禁止
- 但書：因業務需求且無其他替代方案者，專案使用

資安法修訂-重點2強化納管機關資安管理(續)

(2)公務機關：強化聯防體系，分層監督管理模式調適

問題

無上級機關之公務機關，依現行法無外部稽核機制

- ✓ 中央：府會五院
- ✓ 地方：直轄市政府、縣(市)政府、地方議會、直轄市山地原住民區公所、直轄市山地原住民區民代表會，鄉（鎮、市）公所、鄉（鎮、市）民代表會

修正重點：

資安署擴大稽核範圍

資安署得**稽核所有**納管機關

強化地方聯防

直轄市山地原住民區公所、直轄市山地原住民區民代表會，鄉（鎮、市）公所、鄉（鎮、市）民代表會之資安管理，由直轄市、縣政府分層監管。

外部稽核結果

上級機關稽核後，將稽核結果送至資安署，上級機關與資安署可要求受稽機關說明或調整。

資安法修訂-重點3精進資安人力策略

■資安人員管理：支援、配置及獎懲

NEW
新增條文

公務機關

調度支援

遇有重大資安事件，得調度各級機關資通安全人員支援，並視為在職訓練的一環

適任性查核

涉及國家機密、軍事機密及國防秘密之資通安全業務人員進行相關查核

特定非公務機關

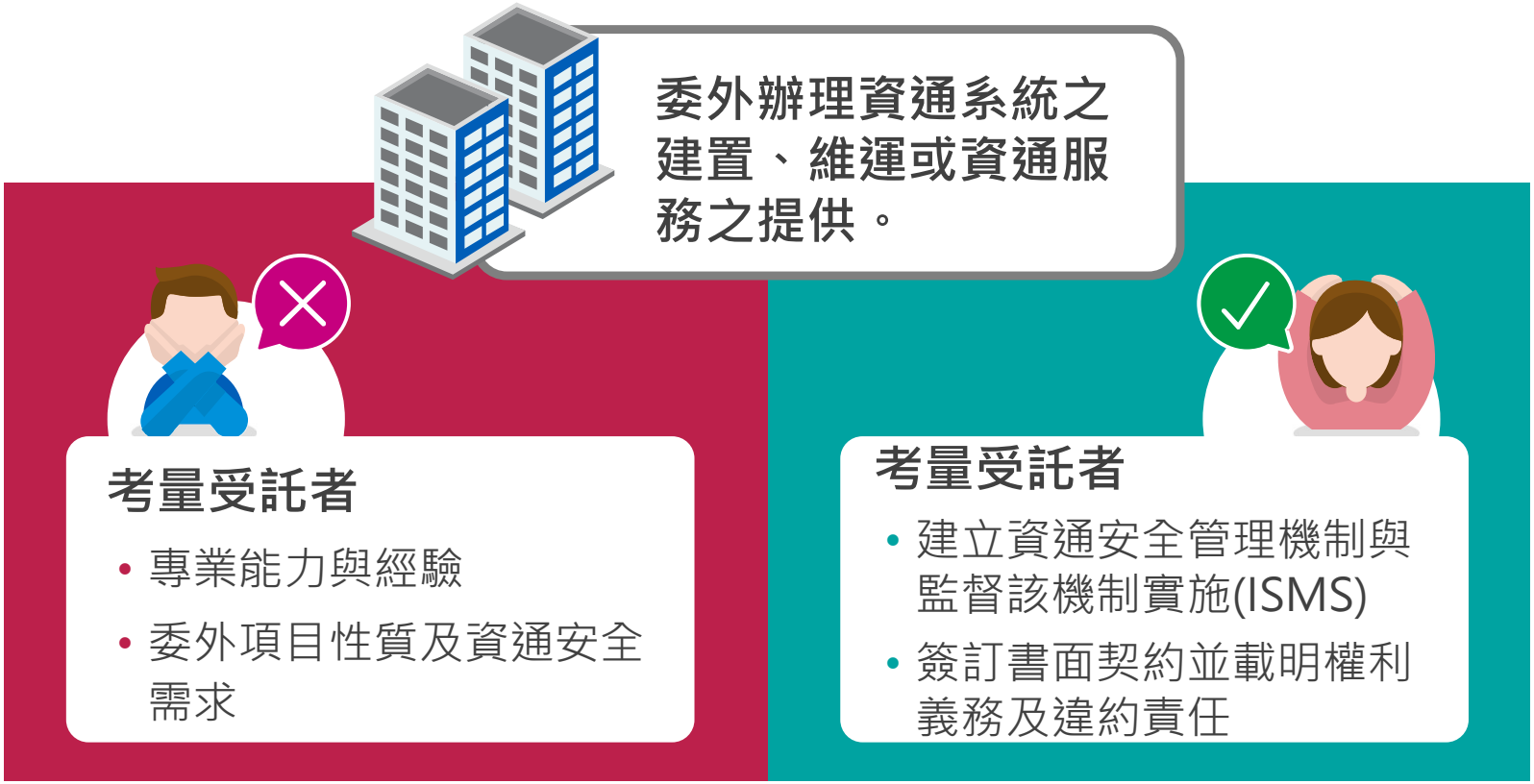
人力配置

應設置專職人員及資安長

獎懲

增訂非公務機關對所屬人員辦理資通安全業務之獎勵及懲處

資安法修訂-重點4委外監督管理機制



資安法修訂-重點5配合通報及應變機制演練授權

公務機關及特定非公務機關應配合辦理資通安全事件通報及應變機制之演練作業授權項目

特定非公務機關之重大資安事件應移送至資安署

通報機關知悉重大資通安全事件時，主管機關或資安署提供相關協助。適當時機並得公告與事件相關之必要內容及因應措施

資安法修訂-授予調查重大資安事件權力

NEW
新增條文

程序

中央目的事業主管機關為調查特定非公務機關發生重大資安事件遵循以下程序與相關罰則

一、通知當事人或關係人到場陳述意見。

二、通知當事人及關係人提出獨立第三方機構出具之鑑識或調查報告。

三、派員、委任或委託其他機關(構)前往當事人及關係人處實施必要檢查，受調查者不得規避、妨礙或拒絕，且不得洩漏知悉非特定公務機關之秘密。

- 執行調查之人員應出示有關執行職務之證明文件，其未出示者，受調查者得拒絕之。
- 違反第二十五條第三項規定，規避、妨礙或拒絕者，由中央目的事業主管機關開處新臺幣十萬元以上一百萬元以下罰鍰。

資安法修訂-附則

三十二條

- **資安署**得委託其他公務機關辦理國家資通安全防護、演練、稽核及其他資通安全事件相關事務。
- 特定非公務機關之業務涉及數個中央目的事業主管機關之權責，**主管機關得協調指定其中一個或數個**中央目的事業主管機關辦理應辦事項。

三十三條

- 資通安全事件涉及個人資料洩漏，應另依個人資料保護法及其相關法令規定辦理。

NEW
新增條文

校園資安訪視常見議題

校園資安訪視重點事項—資通安全維護計畫

- 每年須檢視與更新(依教育局頒布版本)
- 校務行政系統帳號及權限清查(下半年度重點)
- 依規定定期執行資訊資產盤點與風險評鑑
- 依資通安全維護計畫之管理審查會議議題進行討論
- 委外廠商或外部人員簽署保密切結文件

校園資安訪視重點事項—監視設備

- 定期檢視韌體更新
- 建立校時機制
- 設定登入帳號的密碼複雜度
- 建立調閱申請機制
- 影像紀錄建議保存1個月以上
- 監視器位置建議建立表單控管，以利快速查閱
- 如有連結網路建議設置於內網(10網段)

校園資安訪視重點事項—儲存裝置(NAS)

- 韌體更新
- 用不到的服務建議移除或關閉
- 啟動防毒軟體
- 預設admin停用，避免共用帳號
- 啟動密碼原則
- 系統帳號權限定期清查
- 如有連結網路建議設置於內網(10網段)

校園資安訪視重點事項—機房與電腦教室

- 設立門禁機制且於門口或走廊設置監視器
- 設置2部空調設備，並定時切換使用
- 設置氣體式滅火器
- 設置防雷擊與電力突波裝置，並設置穩壓器
- 機房建置設備變更管理機制

校園資安訪視重點事項—其他(1/2)

- 主管、行政及教職人員均須接受3小時資安通識教育訓練
- 內部設備建議盡量設置於內部網段(10網段)
- 注意網路印表機掃描連線設定方式
- 學校跑馬燈之控制PC勿與網路連線
- 勿使用大陸廠牌產品

校園資安訪視重點事項—其他(2/2)

使用Shadon檢查外部網路設備情形

不再使用之DNS紀錄建議刪除

113年學校資安訪視共通事項(1/4)

項目	共同發現事項
資通安全維護計畫	管理審查會議未依資安維護計畫之管理審查議題進行討論。
	未使用最新版本資通安全維護計畫
	監視設備或影印機廠商工程師之到校服務廠商工程師，未簽署保密切結書。
個人電腦	常用安裝軟體如：7-zip須更新至最新版本。(目前為24.X版)
	學校於門口之跑馬燈或大屏螢幕，控制更新之PC建議單獨連線，勿可以上網。

資通安全維護計畫-管理審查討論議題(1/2)

(1)與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

(2)資通安全維護計畫內容之適切性。

(3)資通安全績效之回饋，包括：

A.資通安全政策及目標之實施情形。

B.人力及資源之配置之實施情形。

C.資通安全防護及控制措施之實施情形。

D.不符合項目及矯正措施。

(4)風險評鑑結果及風險處理計畫執行進度。

資通安全維護計畫-管理審查討論議題(2/2)

(5)資通安全事件之處理及改善情形。

(6)利害關係人之回饋。

(7)持續改善之機會。

(8)其他。

113年學校資安訪視共通事項(2/4)

項目	共同發現事項
監視錄影設備	監視錄影主機未設定自動校時(建議設置教網校時伺服器IP)或定期執行人工校時，以確保影像紀錄之有效性；並於「監視錄影系統保養紀錄表」中建議增設「校時檢查」欄位。
	監視系統管理者帳號密碼資訊勿記憶於系統上，使用完畢後應立即登出；勿使用廠商預設密碼且須定期更換。
	已設置監視錄影系統保養紀錄表但尚未進行填寫。

- 監視器自動校時設定，請設定到教網的時間伺服器：163.20.254.254 以避免佔用對外之網路頻寬

113年學校資安訪視共通事項(3/4)

項目	共同發現事項
網路儲存裝置	未設定密碼原則及定期變更密碼。
	未安裝防毒軟體，並且未設定執行定期排程掃毒。
	建議應避免共用帳號，並須定期清查使用者帳號。
多功能事務機	多功能事務機掃描功能使用FTP或網路磁碟設定，但設定帳號或權限不安全。
	建議學校影印機租賃契約增加要求廠商須遵循本校資通安全規範之條款。

- 建議學校逐漸將儲存裝置汰除，資料儲存逐漸移轉至Google或微軟的雲端服務
- 不需要使用之設備建議關閉電源並移除網路，以節省電源及避免被入侵

常見多功能事務機掃描功能設定問題

- 以FTP 方式
  - 問題1：於PC端安裝ftp常駐程式，開啟ftp常駐程式，檢查帳號設定，可以看到帳號是否有設定密碼
  - 問題2：在PC DOS介面，打以下指令，檢查是否有將匿名登入關閉
    >ftp PC-IP
    >user anonymous
  - 如可以不需打密碼登入，則表示未關閉匿名登入
- 以網路芳鄰方式
  - 在其設定掃描資料夾上，按右鍵點選”內容”，點選”安全性”，檢查其權限設定，如有設定”Everyone”，表示只要知道PC的IP，即可透過網路芳鄰的方式連線該資料夾，掃描的資料可以被未授權人員看到

113年學校資安訪視共通事項(4/4)

項目	共同發現事項
機房暨電腦教室	學校機房與電腦教室未放置滅火器或放置乾粉滅火器，建議應放置氣體式滅火器(CO2、環保氣體)。
	重要電腦設備場所門口(如：資訊組、電腦教室等)建議設置監視器，以防發生事件可供調閱。

- 機房不斷電系統(UPS)如果使用多年，建議進行汰換，以免發生火災。
- UPS汰換的電池勿堆放於機房，以免發生自燃產生災情

乾粉滅火器

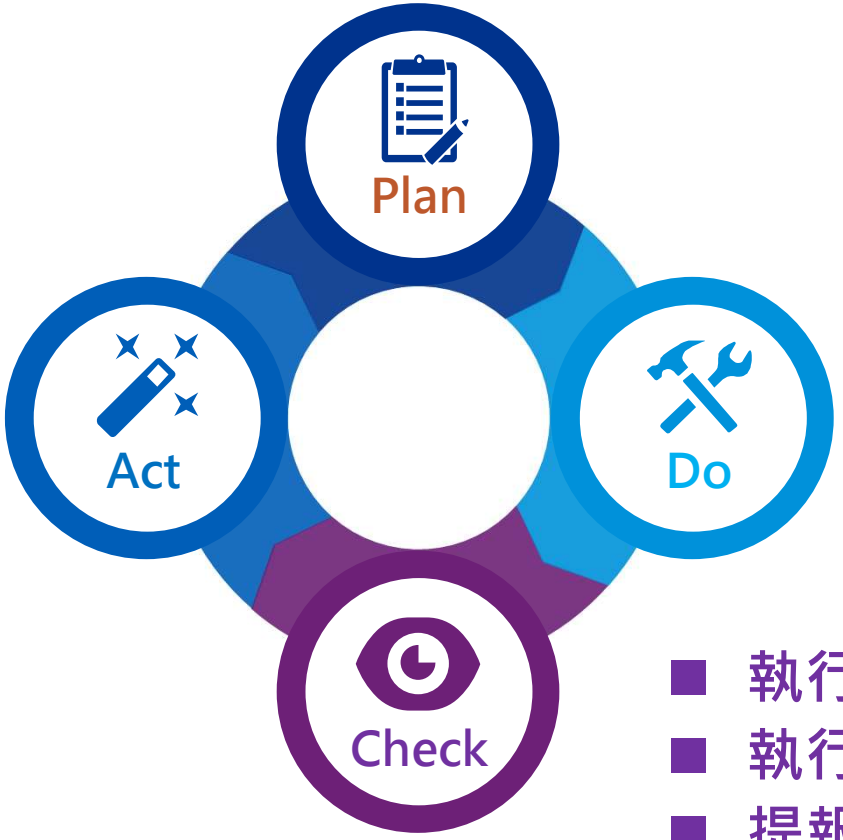
CO2滅火器
(須每年秤重)

環保氣體滅火器
(永久有效)

如何做好校園資通安全管理

資通安全管理法落實方式

- 訂定資安維護計畫
- 執行資訊資產盤點作業
- 執行風險評鑑與處理作業
- 執行資通系統分級與防護基準評估



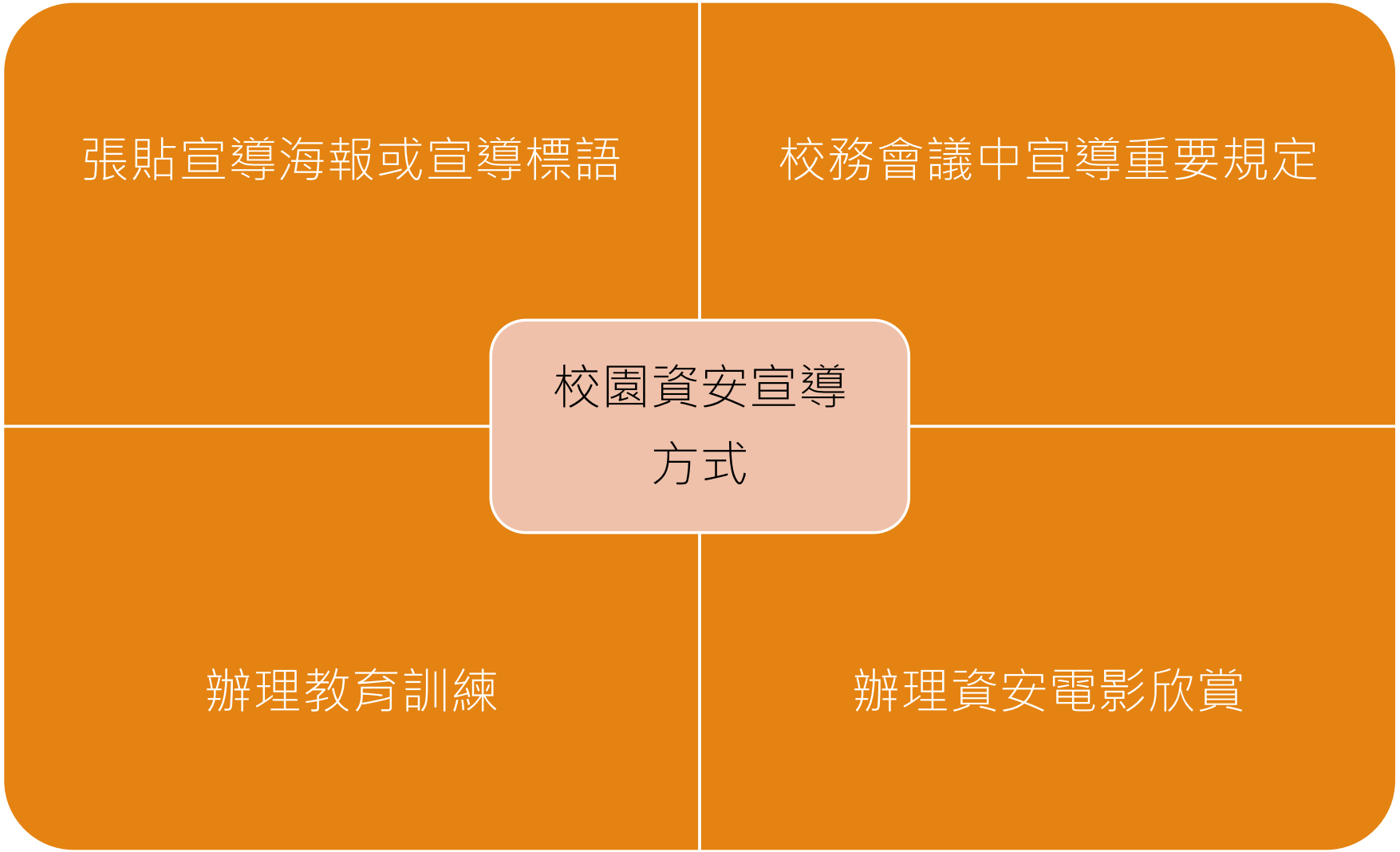
- 執行改善措施

- 執行「資安責任等級分級辦法」之各項應辦事項
- 執行資通安全防護及控制措施
- 執行資安事件通報與應變機制

- 執行資通安全內部稽核作業
- 執行委外廠商稽核或監督
- 提報資安維護計畫實施情形

51

校園內資安宣導執行方式



資安電影參考

- 神鬼駭客：史諾登
- 全民公敵
- 黑帽駭客
- 沒有絕對安全的系統(who am I)
- 原本以為只是手機掉了
- 第四公民
- 直播風暴
- 視界戰(Anon)

電腦機房管理

- 機櫃線路標示
- 機櫃線路盡量整理，線路或電線勿跨地板架設
- 汰換之電池或不斷電設備物堆置於機房內
- 電腦機房勿堆放紙箱或其他易燃物
- 機房內空調機盡量使用2部輪流切換使用(盡量用2部1對1分離式空填或窗型空調)
- 機房未授權人員進出應留下紀錄
- 機房設備有異動應留下紀錄
- 設置氣體式滅火器
- 門口應有門禁措施，走廊應有監視器監視機房門口

電腦教室管理

- 電腦教室門口應有監視器監視門口
- 電腦教室應有門禁措施
- 電腦教室應設置穩壓設備
- 電腦教室內應設置氣體式滅火器

資訊資產盤點與風險評鑑

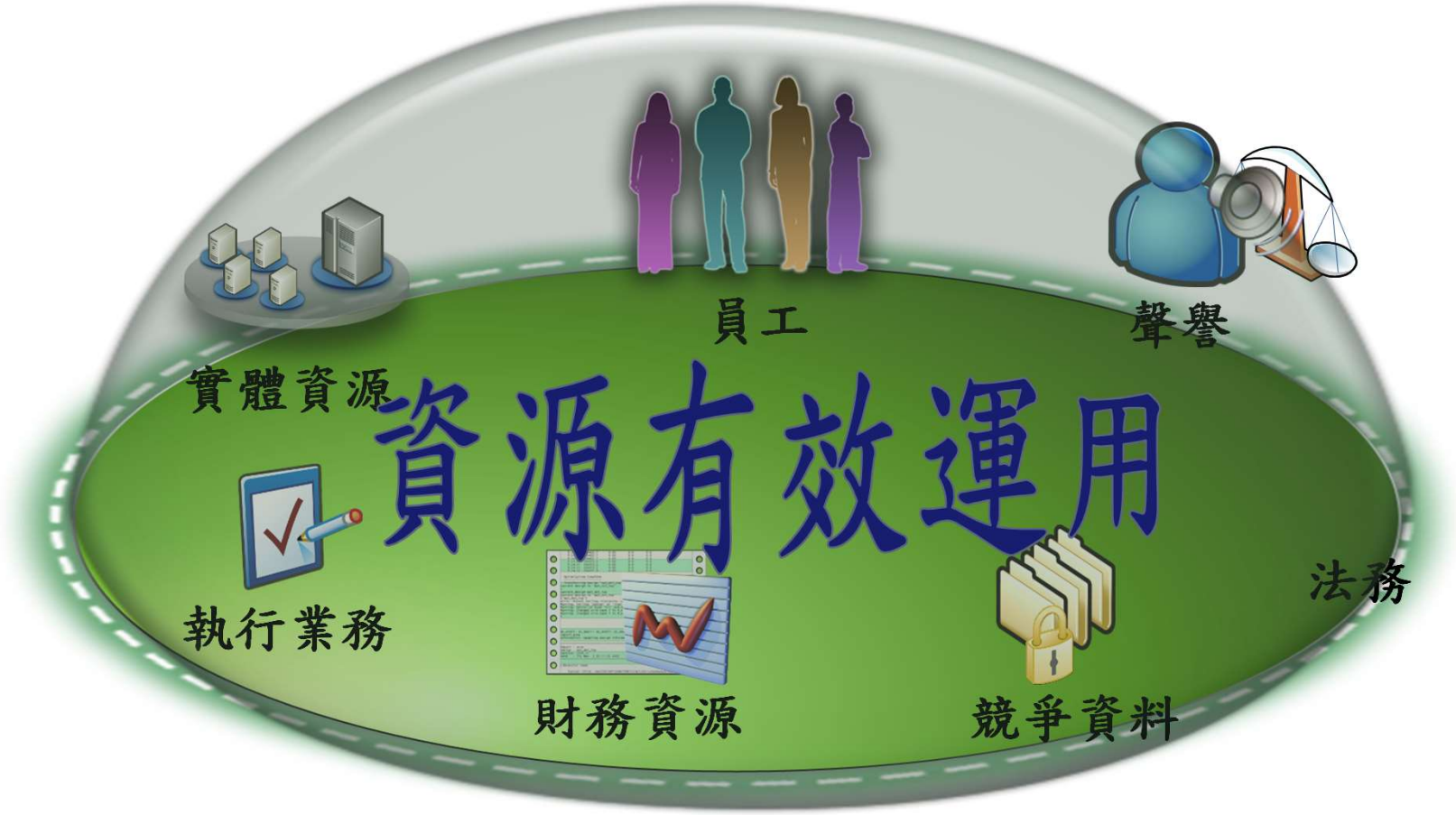
- 參考資通安全維護計畫附件，盤點學校內之資訊資產
- 參考資通安全維護計畫附件，針對資訊資產執行風險評鑑與風險處理作業

學校為什麼需要風險管理?

- 對組織
  - 保護資訊資產
  - 問題管理
  - 資源分配
- 對個人
  - 取得資源
  - 保護自己

風險管理的效益

- 識別資產– 我需要保護什麼?
- 識別風險–我需要採取何種對策?
- 計算風險–需要多少時間、人力、或成本來保護重要資產?



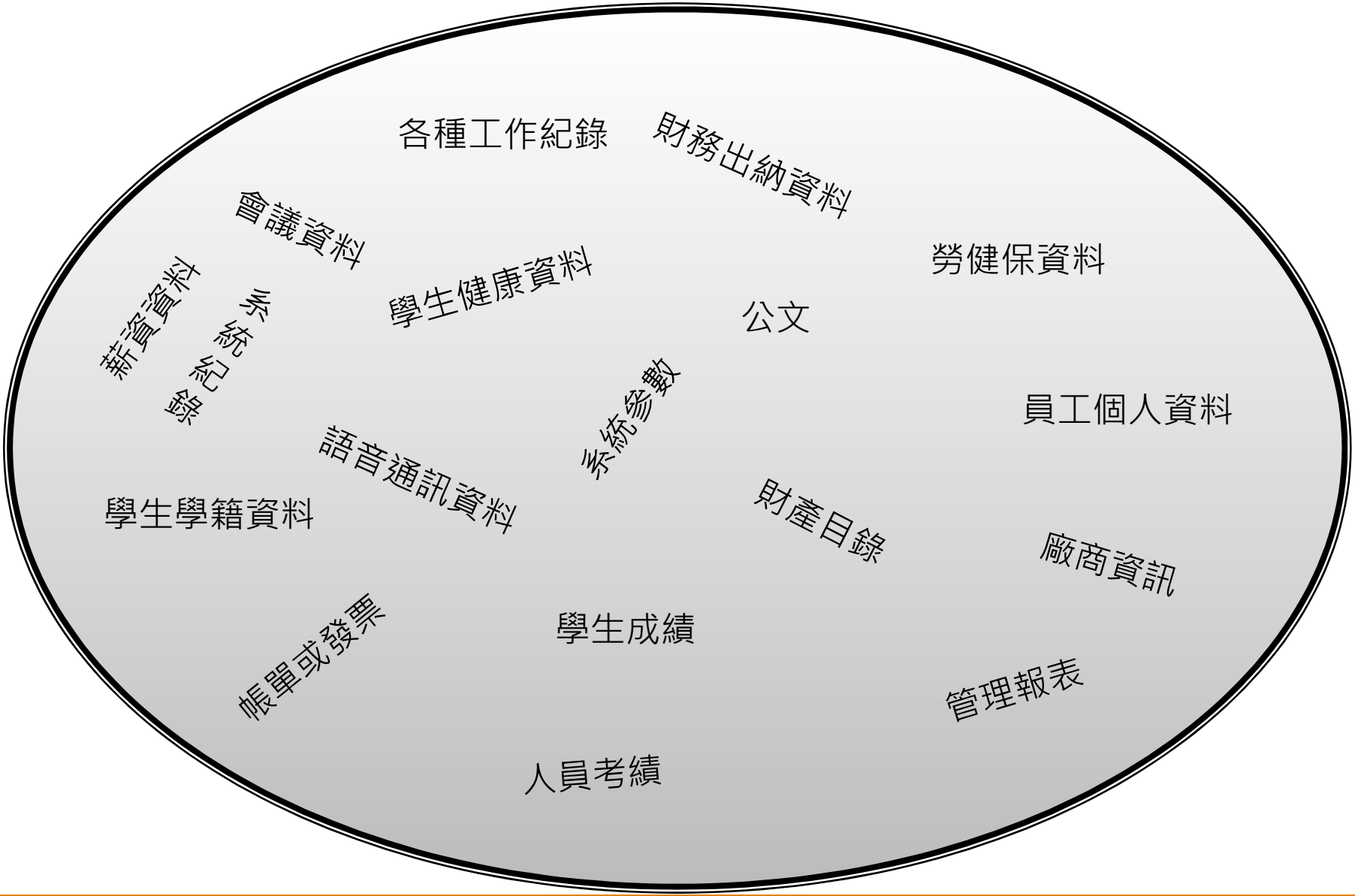
何謂資訊?

- **資訊**
  - 任何型態顯示及任何媒體儲存經處理過之資料
- **價值**
  - 資訊內容
- **存在方式**
  - 紙本
  - 伺服器
    - 檔案
    - 資料庫
  - 網路

資訊形式

- 電腦相關資訊
- 正式文件
- 文件草稿
- 工作文件
- 信手塗鴉
- 內部通訊
- 法律及規範檔案
- 其他紀錄
- 媒體及開放來源
- 正式會議
- 非正式會議
- 閒聊漫談

學校內資訊種類


各種工作紀錄
財務出納資料
會議資料
薪資資料
學生健康資料
勞健保資料
公文
員工個人資料
語音通訊資料
學生學籍資料
財產目錄
廠商資訊
帳單或發票
學生成績
管理報表
人員考績

資訊資產盤點與風險評估執行流程

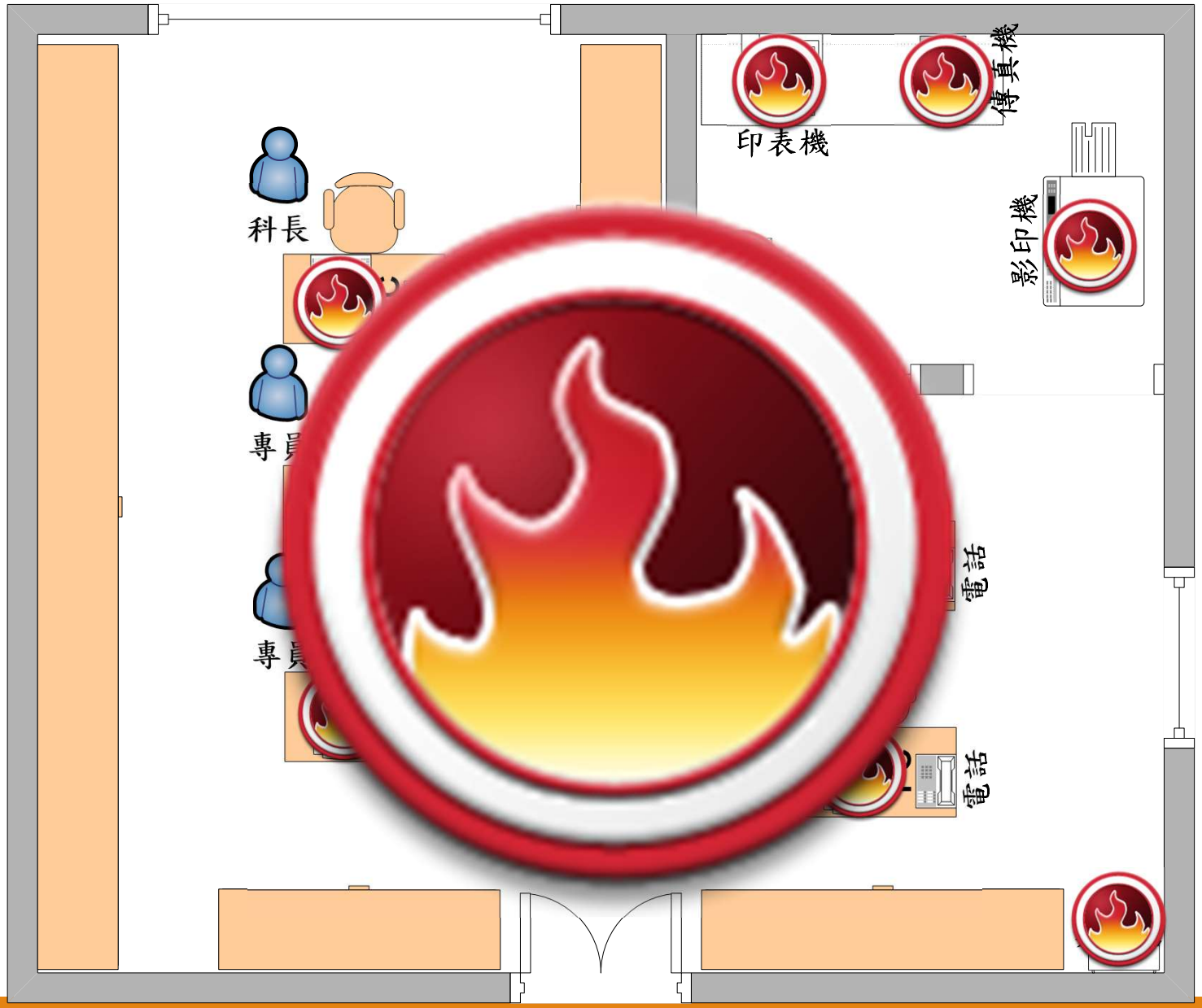
1.盤點資訊資產與分類

- 依據學校資通安全維護計畫執行
- 資訊資產類別分為：資訊資產、實體資產、軟體資產、人員資產、資料資產、支援服務資產

資訊資產類別

- 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等
- 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等
- 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等
- 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等
- 人員資產：內部設備維運管理人員、主管、使用人員，以及委外廠商駐點人員等
- 資料資產：以紙本形式儲存之資訊，如程序、清單、計畫、報告、指引手冊、政策、公文、作業紀錄、作業規範、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等

資訊資產的分類將影響風險的識別-1/2

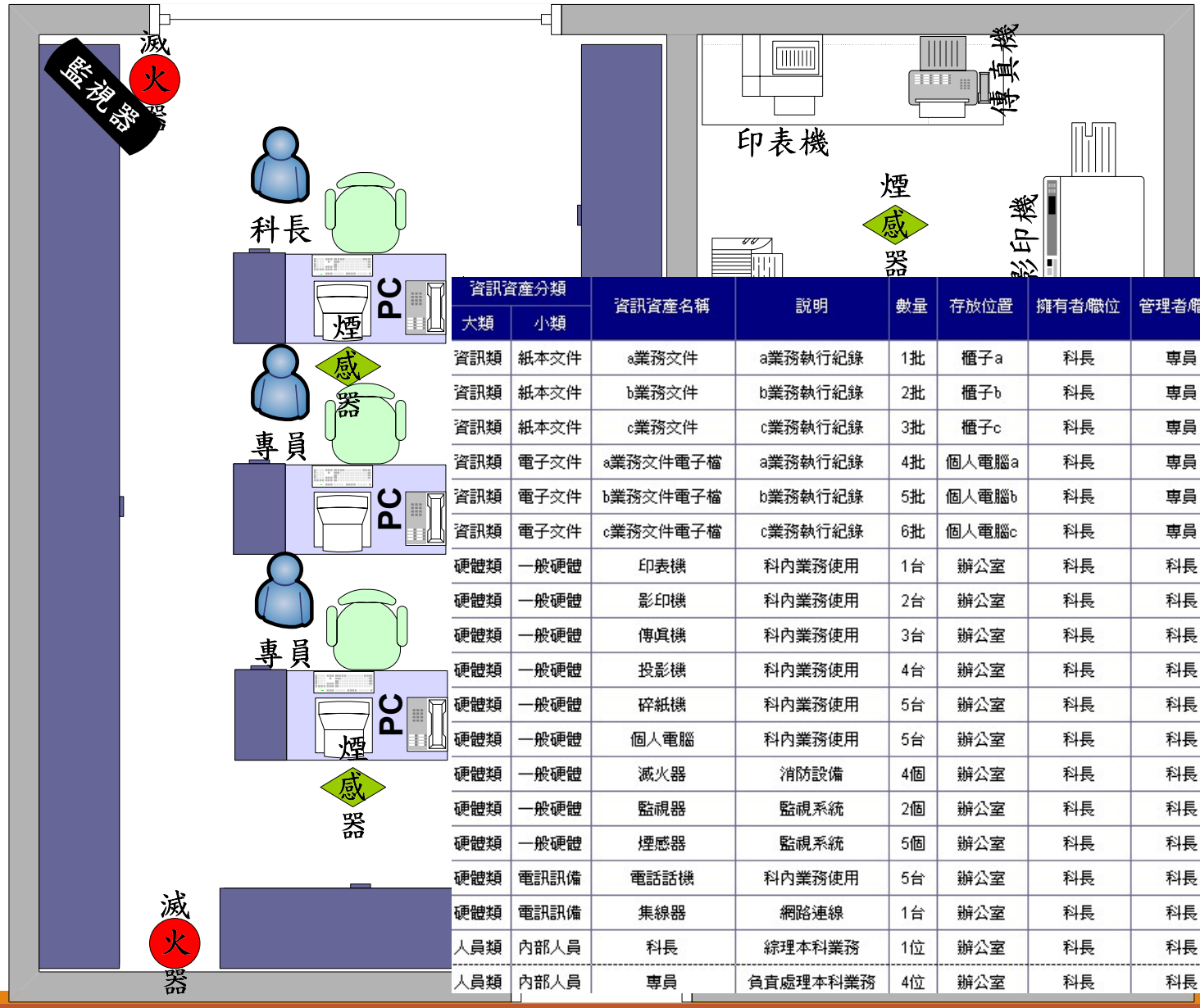


資訊資產的分類將影響風險的識別-2/2

資訊資產盤點的方式

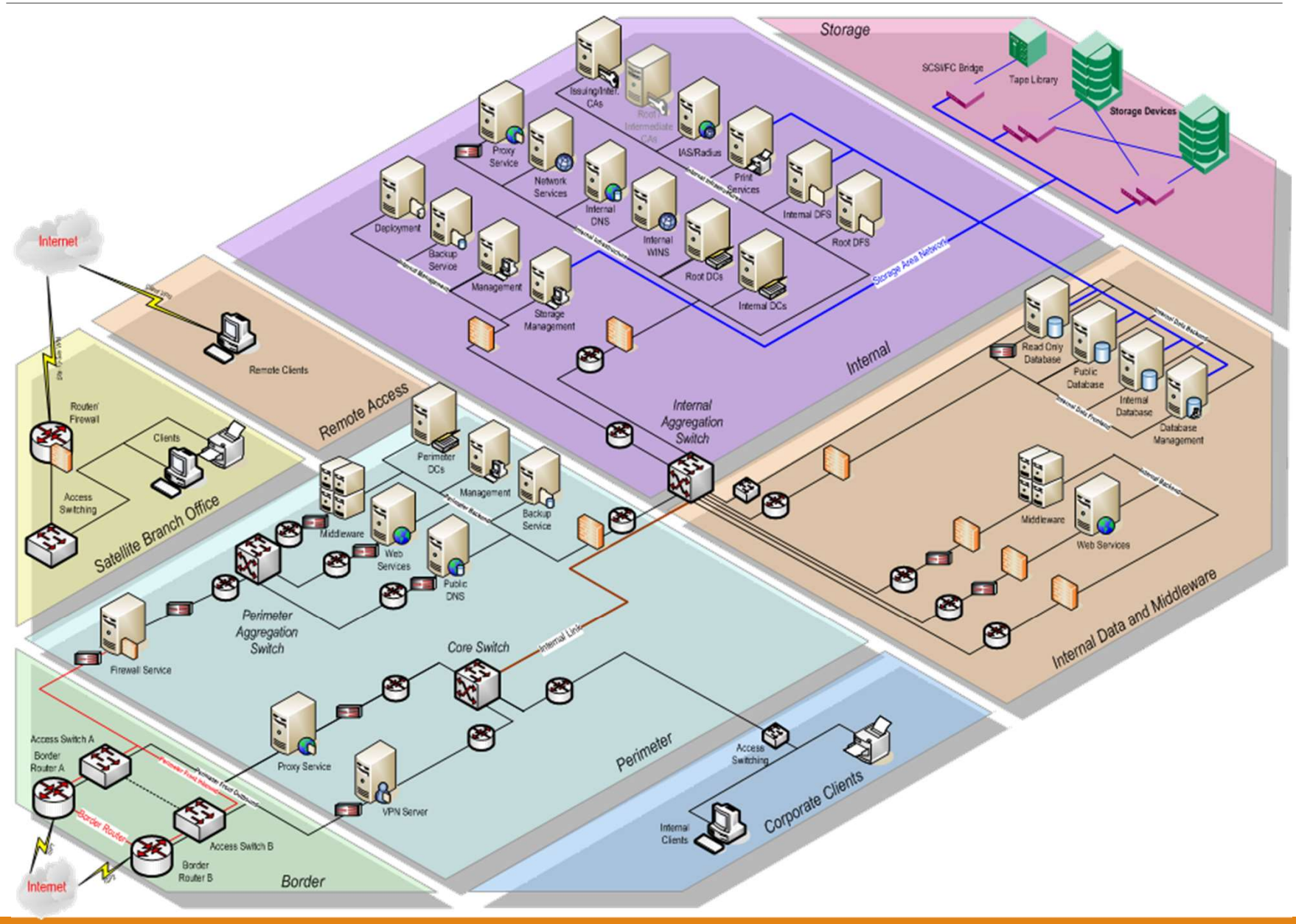
- 面
  - 實體環境配置
  - 網路架構圖
  - 資產管理系統(硬體、軟體)-財產帳
- 線
  - 作業流程圖
  - 系統的資訊資產關連圖
- 點
  - 個人工作職掌
  - 伺服器、個人電腦

實體環境配置



資訊資產分類		資訊資產名稱	說明	數量	存放位置	擁有者/職位	管理者/職位	使用者(部門)
大類	小類							
資訊類	紙本文件	a業務文件	a業務執行紀錄	1批	櫃子a	科長	專員	資訊科
資訊類	紙本文件	b業務文件	b業務執行紀錄	2批	櫃子b	科長	專員	資訊科
資訊類	紙本文件	c業務文件	c業務執行紀錄	3批	櫃子c	科長	專員	資訊科
資訊類	電子文件	a業務文件電子檔	a業務執行紀錄	4批	個人電腦a	科長	專員	資訊科
資訊類	電子文件	b業務文件電子檔	b業務執行紀錄	5批	個人電腦b	科長	專員	資訊科
資訊類	電子文件	c業務文件電子檔	c業務執行紀錄	6批	個人電腦c	科長	專員	資訊科
硬體類	一般硬體	印表機	科內業務使用	1台	辦公室	科長	科長	資訊科
硬體類	一般硬體	影印機	科內業務使用	2台	辦公室	科長	科長	資訊科
硬體類	一般硬體	傳真機	科內業務使用	3台	辦公室	科長	科長	資訊科
硬體類	一般硬體	投影機	科內業務使用	4台	辦公室	科長	科長	資訊科
硬體類	一般硬體	碎紙機	科內業務使用	5台	辦公室	科長	科長	資訊科
硬體類	一般硬體	個人電腦	科內業務使用	5台	辦公室	科長	科長	資訊科
硬體類	一般硬體	滅火器	消防設備	4個	辦公室	科長	科長	資訊科
硬體類	一般硬體	監視器	監視系統	2個	辦公室	科長	科長	資訊科
硬體類	一般硬體	煙感器	監視系統	5個	辦公室	科長	科長	資訊科
硬體類	電訊訊備	電話話機	科內業務使用	5台	辦公室	科長	科長	資訊科
硬體類	電訊訊備	集線器	網路連線	1台	辦公室	科長	科長	資訊科
人員類	內部人員	科長	綜理本科業務	1位	辦公室	科長	科長	資訊科
人員類	內部人員	專員	負責處理本科業務	4位	辦公室	科長	科長	資訊科

網路架構圖


Storage
SCSI/FC Bridge
Tape Library
Storage Devices
Issuing/Inter. CAs
Root / Intermediate CAs
Proxy Service
Network Services
IAS/Radius
Print Services
Internal DNS
Internal WINS
Internal DFS
Root DFS
Deployment
Backup Service
Management
Storage Management
Root DCs
Internal DCs
Storage Area Network
Internet
Remote Clients
Remote Access
Router/ Firewall
Clients
Access Switching
Satellite Branch Office
Internal
Internal Aggregation Switch
Perimeter DCs
Management
Backup Service
Middleware
Web Services
Public DNS
Perimeter Aggregation Switch
Firewall Service
Core Switch
Internal Links
Read Only Database
Public Database
Internal Database
Database Management
Middleware
Web Services
Internal Data and Middleware
Access Switch A
Border Router A
Border Router
Access Switch B
Border Router B
Internet
Border
Proxy Service
VPN Server
Perimeter
Access Switching
Internal Clients
Corporate Clients

個人工作職掌

XX單位-網路管理組(範本)

姓名	職稱	工作職掌	辦公地點
林志玲	網路管理組組長	1.綜理全組業務 2.網路管理組工作協調與追蹤 3.規劃網路管理組服務品質之提昇 4.其他交辦事項	教網中心 A221
皮卡丘	技士	1.預算使用管理 2.OA辦公室自動化系統收發文處理 3.本校網路相關問題管理 4.工讀生管理 5.撥接線路及專線繳費處理 6.協助解決職員之網路使用問題 7.財產保管 8.其他交辦事項	教網中心 A221

2.評估資訊資產價值

- 資產價值取機密性、完整性與可用性之最大值

評分 / 類型	0	1	2	3
機密性(C)	無此特性或可公開	僅供單位內部人員使用	僅供業務相關人員存取	具特殊權限人員方可存取
完整性(I)	無此特性或不影響單位運作	將造成本校部份業務運作效率降低	將造成本校部份業務運作停頓	將造成本校大部分業務運作停頓
可用性(A)	無此特性或最大可容忍中斷時間5天以上	最大可容忍中斷時間3天以上，5天以下	最大可容忍中斷時間1天以上，3天以下	最大可容忍中斷時間1天以內

3.選擇潛在風險事件

資產大類	資產小類	潛在風險事件	管控措施範例說明
1.軟體資產類	1.1作業系統	1.1.1未落實作業系統更新/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-WSUS機制失效 -定期檢查漏洞更新狀態 -資訊單位定期彙整提供發佈更新資訊，供業務單位進行比對
1.軟體資產類	1.1作業系統	1.1.2未購買妥適的作業系統授權/使用授權超過購買數，致使遭受廠商求償或抗議。	-作業系統授權清單
1.軟體資產類	1.1作業系統	1.1.3未汰換原廠公告停止技術支援之作業系統，進而無法修補漏洞，致使遭受惡意攻擊、資料外洩或其他侵害。	
1.軟體資產類	1.1作業系統	1.1.4未加入組織之網域，進而無法套用GCB或群組原則政策，致使無法有效管控。	-套用GCB設定，或設定適當權組原則
1.軟體資產類	1.1作業系統	1.1.5個人電腦或伺服器等資訊設備未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
1.軟體資產類	1.1作業系統	1.1.6作業系統最高管理權限管制不當，有共用或浮濫設定的情形。	

4.計算風險值

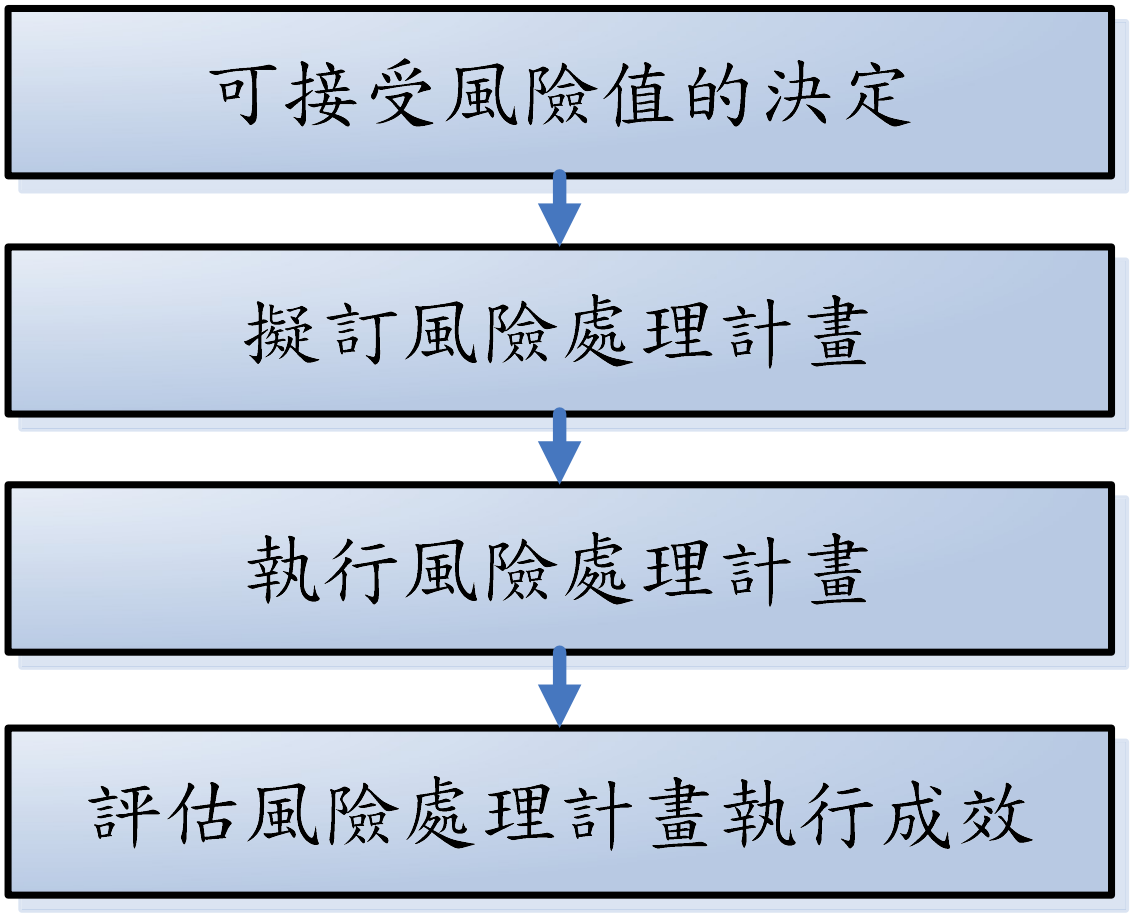
- 評估風險發生可能性

風險發生可能性	數值
高	3
中	2
低	1

- 風險值=資產價值 X 風險發生可能性

5.執行風險處理

- 風險處理(Risk Treatment)-選擇與實施各項控制措施，以修正風險的過程



進行風險處理

- 依據資通安全維護計畫，可接受風險值為6
- 高於可接受風險值的資訊資產，應依據識別的潛在風險進行風險處理計畫的擬訂
- 新增控制措施，降低風險的發生機率
- 將資訊資產的風險值降低至可接受風險值以下

擬訂風險處理計畫

- 風險處理決策
  - 風險減緩：增加控制措施以減少風險及強化資訊安全
  - 風險轉移：轉換風險給其他組織，例如：保險或保修合約
  - 風險迴避：不執行相關活動及避免風險發生的機會
  - 風險承受：不論發生與否均接受風險及吸收相關產生的成本
- 依據風險處理策略，資訊資產保管者擬訂風險處理計畫

監視設備管理

- 監視設備管理帳號應設置具有強度密碼(8碼以上，具有文數字或特殊符號混合)，並由專人保管密碼
- 監視設備如有連線，應設置於內部私有IP網段(192.168.XX.XX)
- 監視設備應設置於安全可監控的位置
- 監視設備影像紀錄建議保存1個月以上
- 監視設備建立校時機制
- 監視器鏡頭建議畫圖標示監控範圍，以利事後調閱
- 定期(建議每周)巡視監視器鏡頭是否正常及監視設備校時與錄影是否正常

校務行政系統帳號及權限管理

- 各類人員帳號原則如下：
  - 教師：由人事室於人員報到後依學校報到流程在於「人事資料管理模組」建立帳號相關資料
  - 學生：由註冊組於學生入學後，至於「學籍管理/學生資料管理模組」建立帳號相關資料。(亦適用於轉學生/復學生)
  - 家長：由家長透過學生帳號申請，或由各班導師於「家長人事管理模組」直接建立帳號相關資料
  - 志工：由輔導處或相關單位依學校報到流程志工保密切結書於「校園志工管理模組」建立帳號相關資料，並要求使其簽署資通安全保密同意書
  - 行政人員：由人事室依學校報到流程到職單於「人事資料管理模組」建立帳號相關資料
  - 其他：由人事室依學校報到流程於「人事資料管理模組」建立帳號相關資料
- 校務行政系統帳號以最小權限為原則
- 校務行政系統帳號依教育局要求，每學年至少清查一次，每個帳號應有對應之使用人員，如無對應使用人員或人員已離職，應刪除該帳號

資通安全推動小組會議審查議題

- 應依「資通安全維護計畫」壹拾伍、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之管理審查議題進行討論

(1) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

(2) 資通安全維護計畫內容之適切性。

(3) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

B. 人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 不符合項目及矯正措施。

(4) 風險評鑑結果及風險處理計畫執行進度。

(5) 資通安全事件之處理及改善情形。

(6) 利害關係人之回饋。

(7) 持續改善之機會。

- 會議後須做成會議紀錄

問題與討論