資通安全管理法通過後
B級/C級學校因應之道

Certification and Business Enhancement 驗證暨企業優化事業群

企業發展與優化服務 產品經理 曾蕙瑜

資通安全管理法介紹

資通安全管理法

資通安全管理法

資通安全管理法施行細則

- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 特定非公務機關資通安全維護計畫實施情形稽核辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法

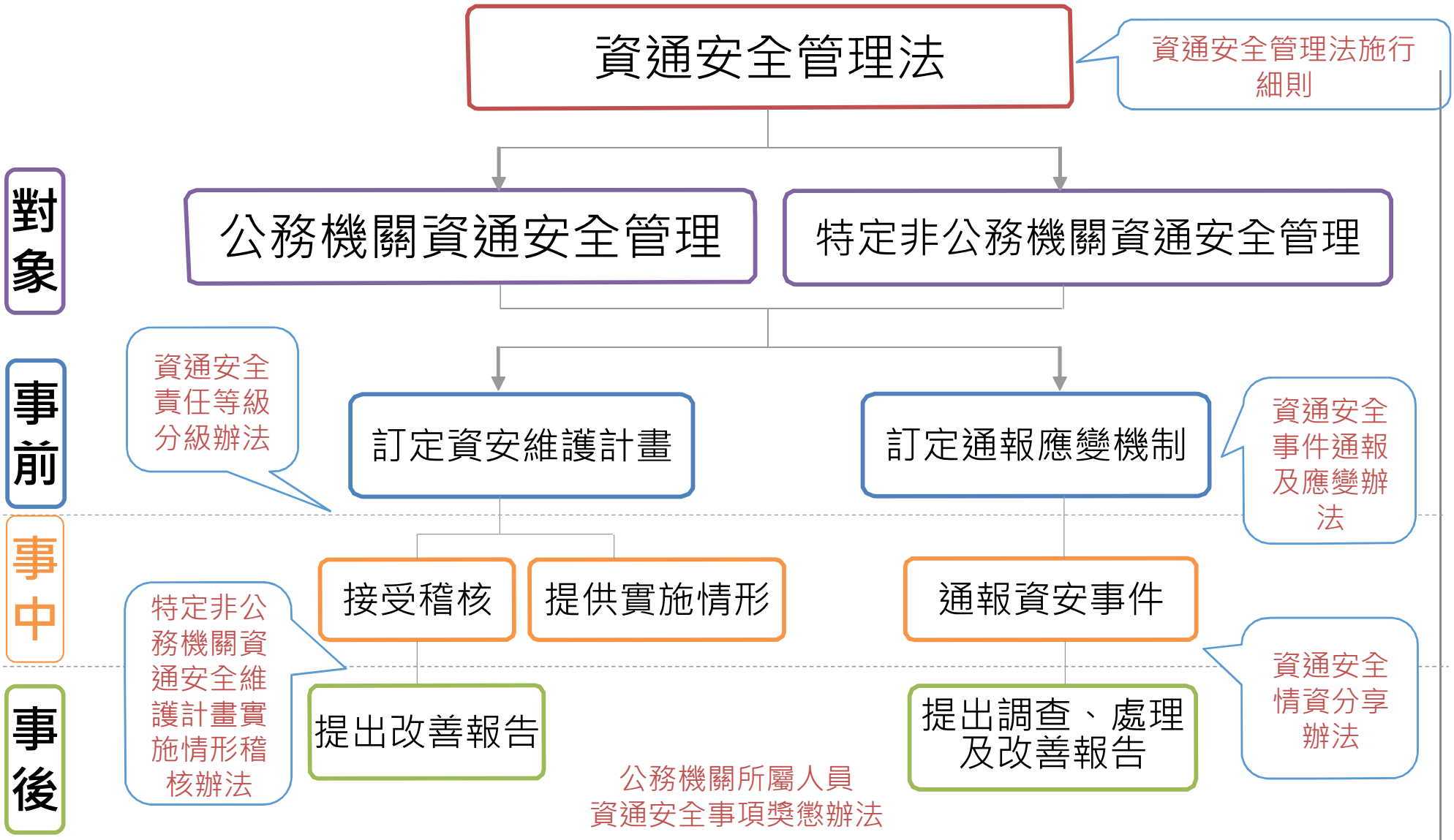
- 資安維護計畫範本
- 公務機關資通安全事件通報應變程序範本
- 特定非公務機關資通安全事件通報應變程序範本

資通安全管理法條文

第一章 總則 第一條~第九條	
第二章 公務機關資通安全管理 第十條~第十五條	第三章 非公務機關資通安全管理 第十六條~第十八條
第四章 罰則 第十八條~第二十一條	
第五章 附則 第二十二條~第二十三條	

立法目的

資安管理法架構


資通安全管理法
資通安全管理法施行細則
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
提供實施情形
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
資通安全情資分享辦法
事後
提出改善報告
提出調查、處理及改善報告
公務機關所屬人員資通安全事項獎懲辦法

5

資通安全管理工作

資通安全管理法工作重點

公務機關

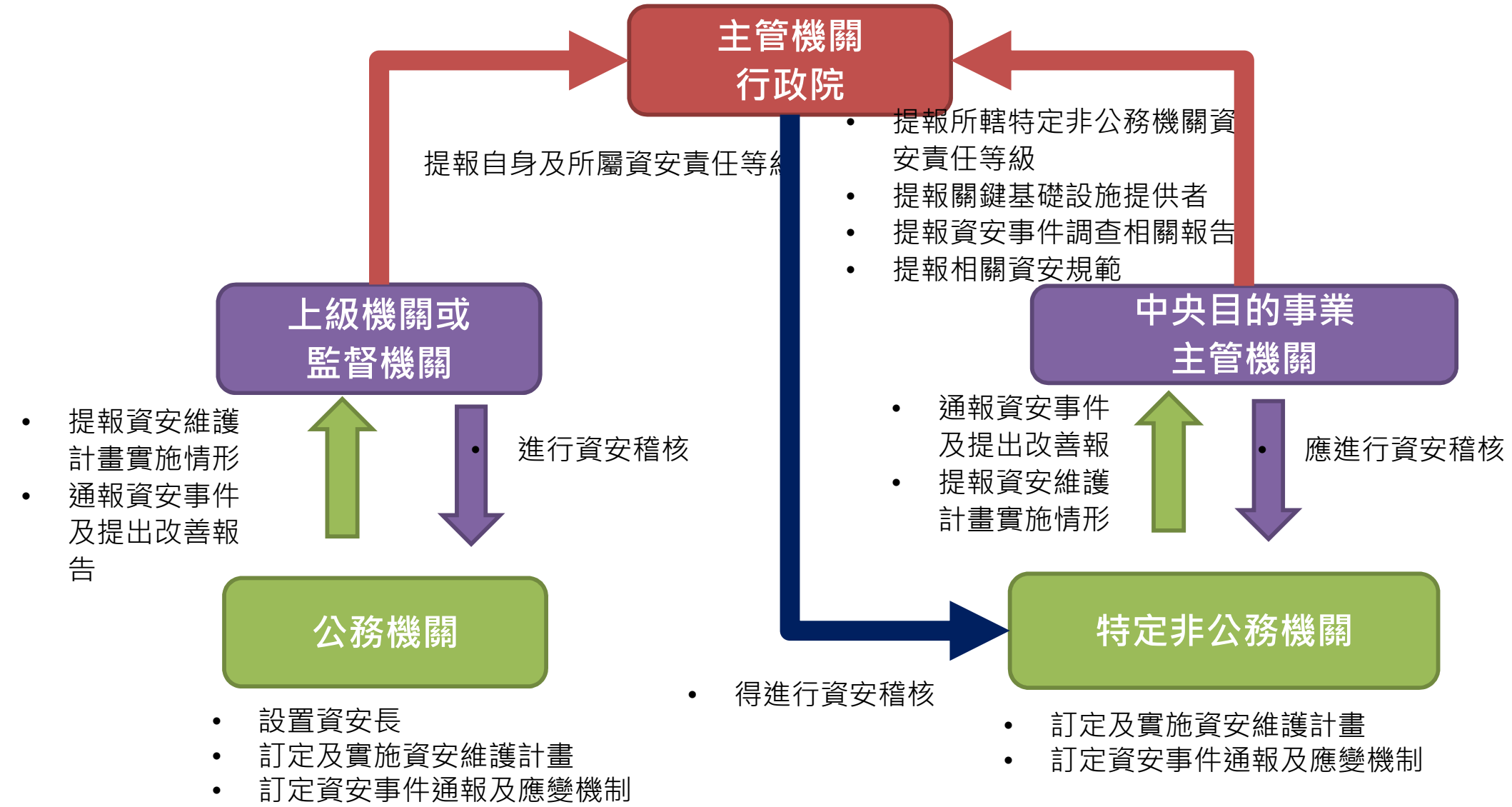
- 中央與地方機關(構)
- 公法人

非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

公務機關			非公務機關		
資安責任等級分級	資安維護計畫	資安長設置	資安責任等級分級	資安維護計畫	年度資安維護計畫實施情形
年度資安維護計畫實施情形	資安稽核	改善報告	資安稽核	資安事件通報應變	改善報告
資安事件通報應變	公務機關人員獎懲標準		公告	罰則	

資通安全管理角色與權責



資通安全管理事項

資通安全責任等級分級辦法

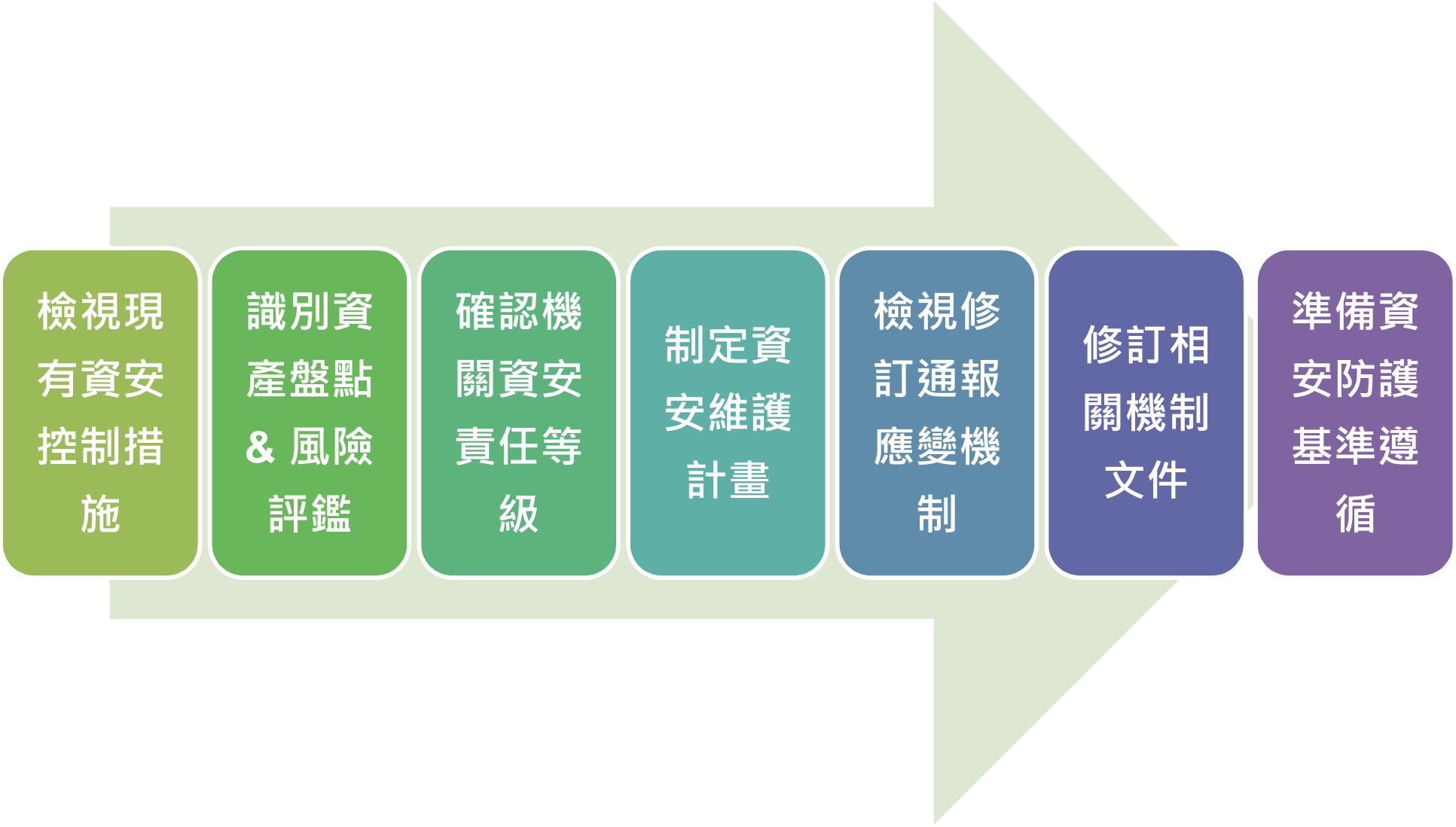
資通安全事件通報及應變辦法

特定非公務機關資通安全維護計畫實 施情形稽核辦法

資通安全情資分享辦法

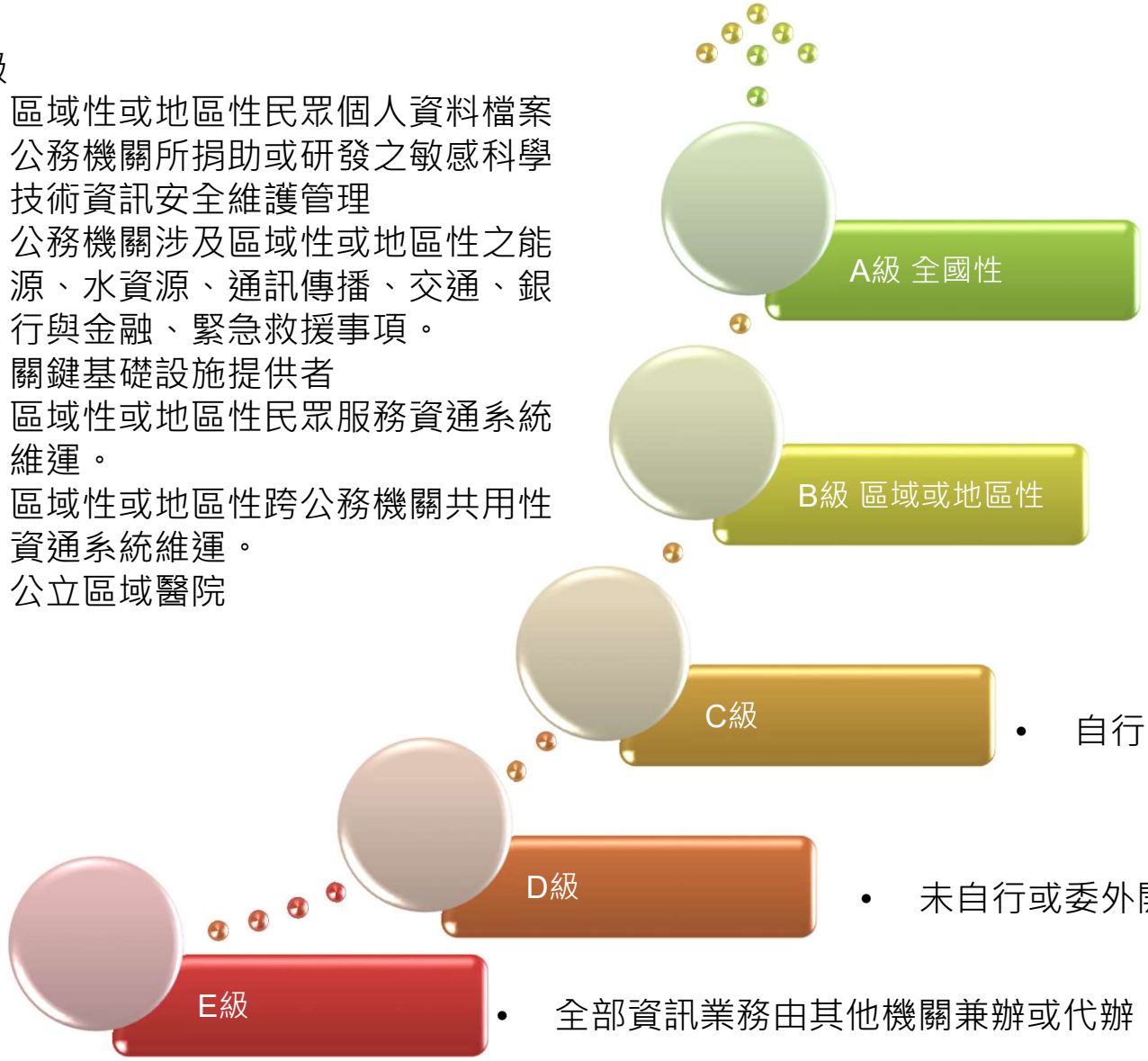
公務機關所屬人員 資通安全事項獎懲辦法

資通安全法準備重點


檢視現有資安控制措施
識別資產盤點 & 風險評鑑
確認機關資安責任等級
制定資安維護計畫
檢視修訂通報應變機制
修訂相關機制文件
準備資安防護基準遵循

資通安全責任等級分級原則

B級
- 區域性或地區性民眾個人資料檔案
- 公務機關所捐助或研發之敏感科學技術資訊安全維護管理
- 公務機關涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。
- 關鍵基礎設施提供者
- 區域性或地區性民眾服務資通系統維運。
- 區域性或地區性跨公務機關共用性資通系統維運。
- 公立區域醫院



A級
- 全國性民眾或公務員個人資料檔案
- 外交、國防或國土安全事項
- 公務機關涉全國性之能源、水、通訊傳播、交通、銀行與金融、緊急救援
- 關鍵基礎設施提供者
- 全國性民眾服務資通系統之維運
- 全國性跨公務機關共用性資通系統之維運
- 公立醫學中心

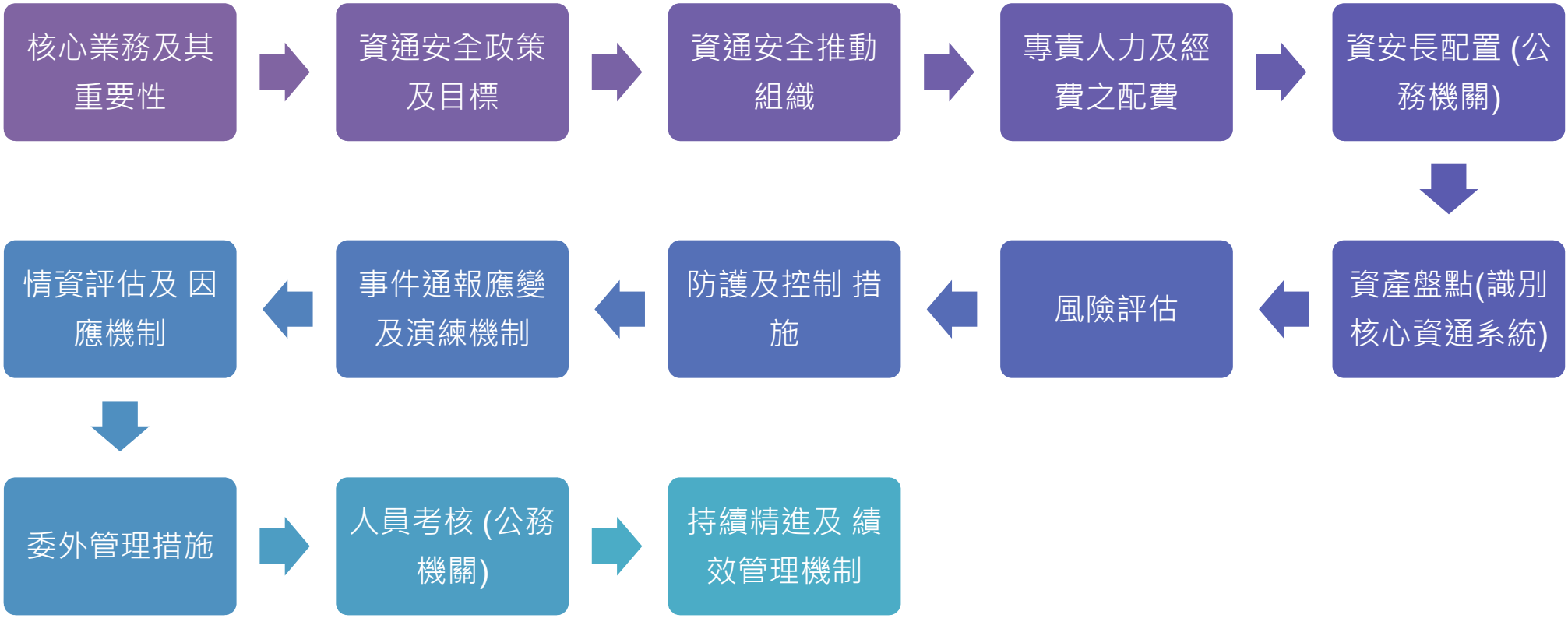
- 自行或委外發資訊系統，並設置伺服器者

- 未自行或委外開發資訊系統，未設置伺服器

- 全部資訊業務由其他機關兼辦或代辦

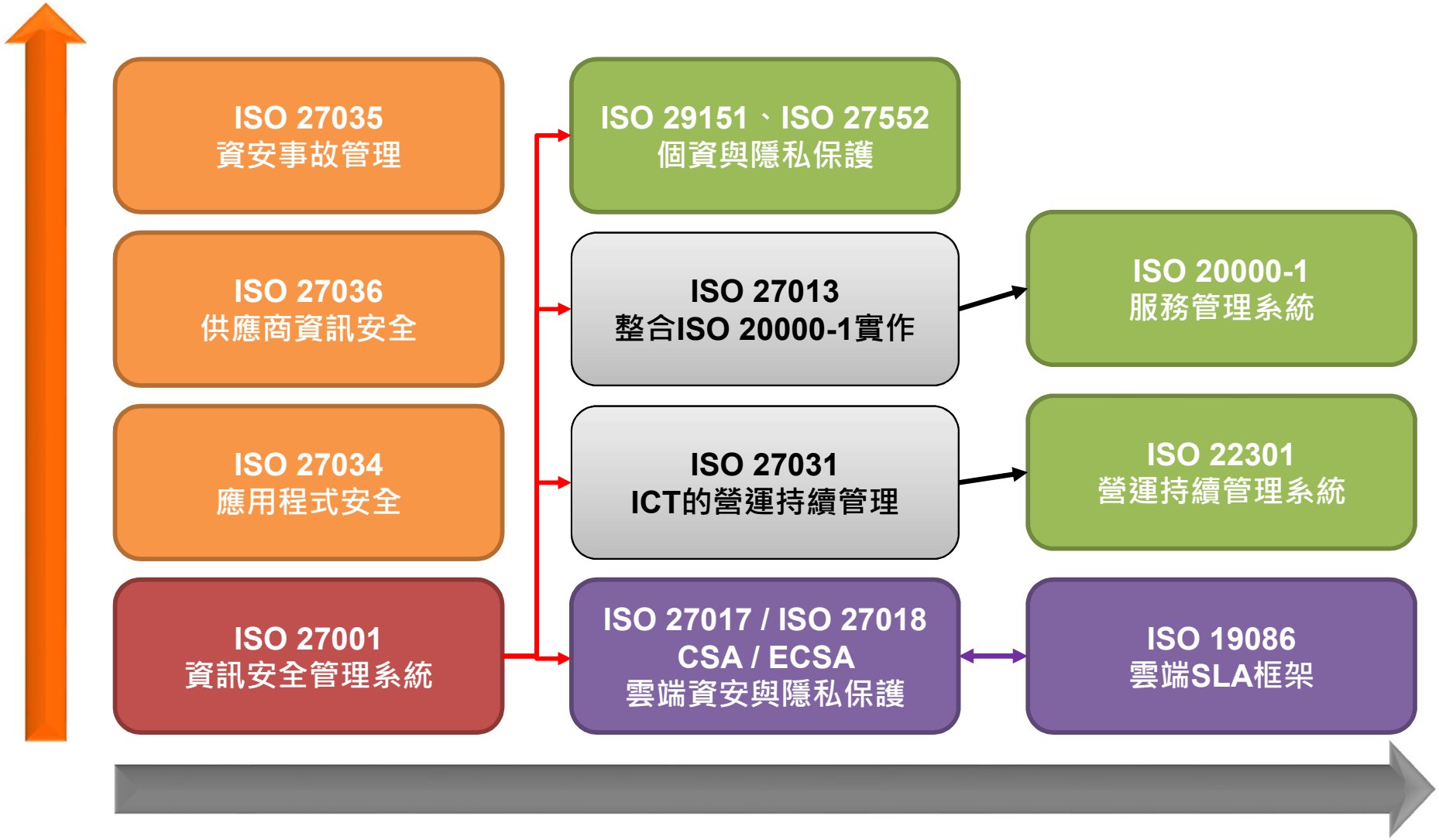
資通安全維護計畫內容

基於風險管理之基礎，包含下列內容



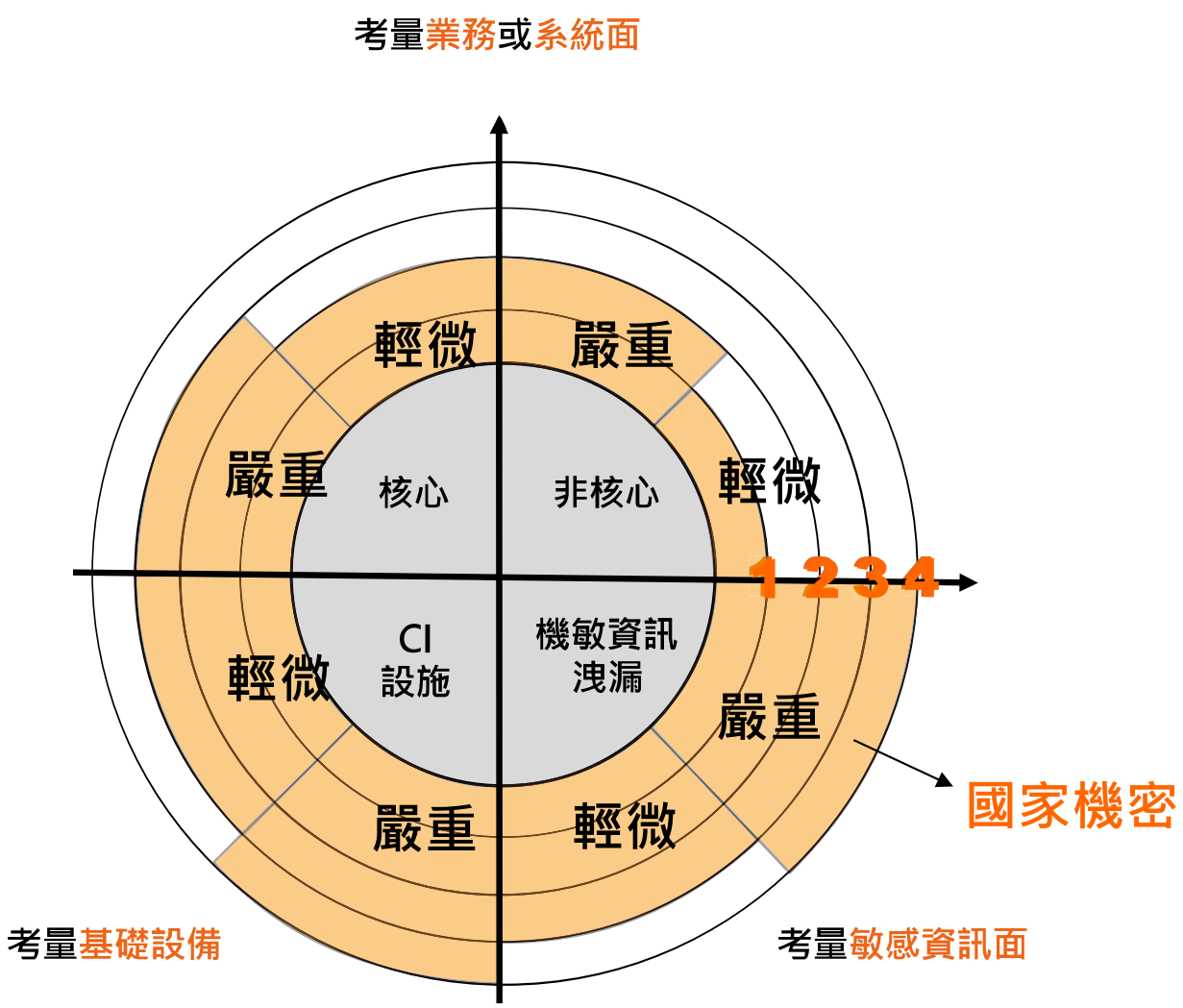
- 維護計畫實施情形，應包括各款之執行成果與相關說明

從ISO 27001開始



資通安全事件通報及應變

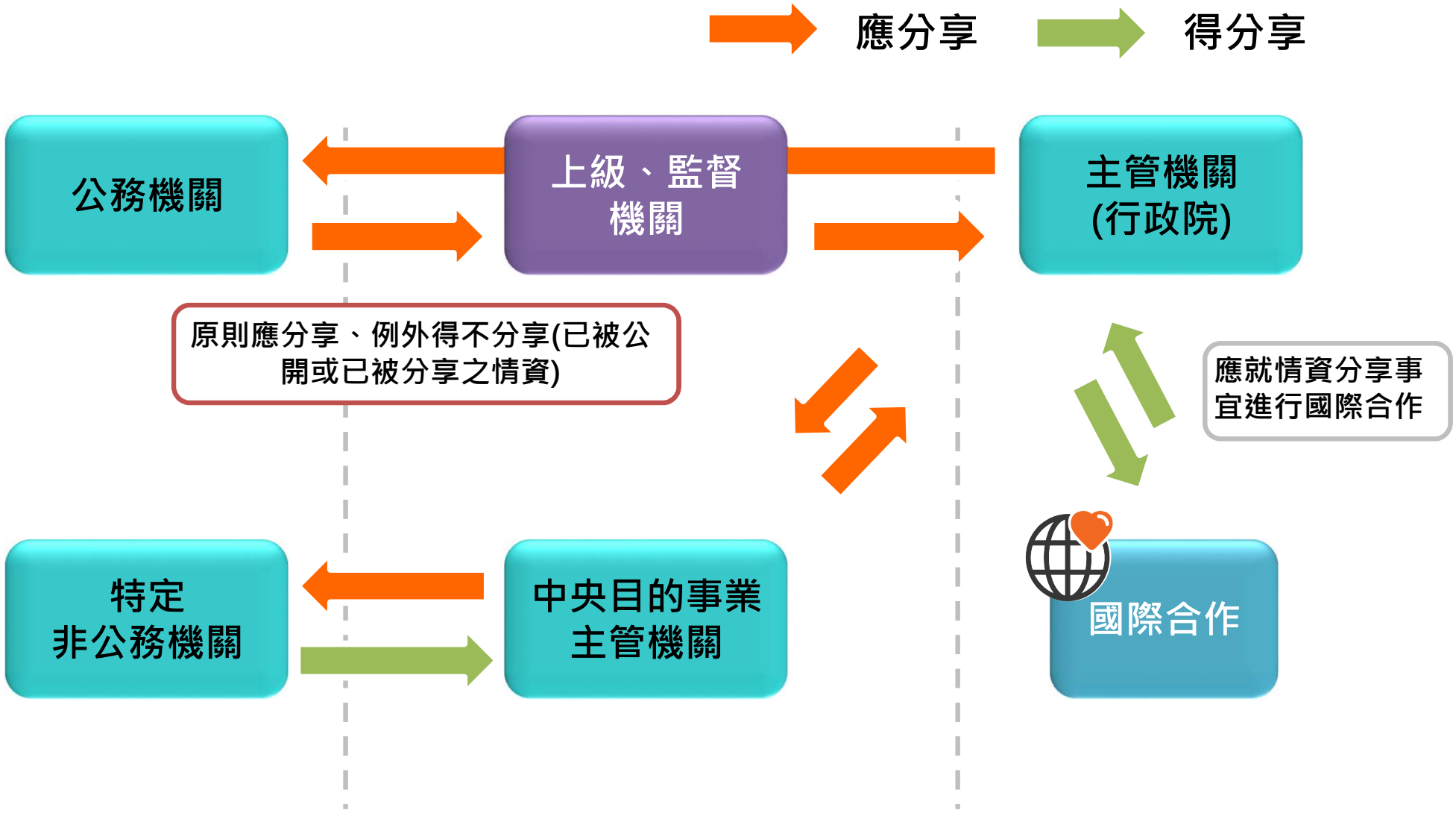
資通安全事件分級



- 事件輕微或嚴重三面向
- 機密性
  1. 業務資訊遭洩漏
- 完整性
  1. 業務資訊遭竄改
  2. 資通系統遭竄改
- 可用性
  1. 資訊系統受影響或停頓，是否於可接受時間內回復

同一資安事件影響二個以上機關，等級向上提升一級。

資安情資分享


應分享
得分享
公務機關
上級、監督機關
主管機關(行政院)
原則應分享、例外得不分享(已被公開或已被分享之情資)
應就情資分享事宜進行國際合作
特定非公務機關
中央目的事業主管機關
國際合作

資安情資內容

1. 惡意偵察/情蒐活動
2. 系統安全漏洞
3. 使安控失效或利用漏洞方法
4. 惡意程式相關資訊
5. 資安事件之損害或影響
6. 偵測、預防或降低損害措施
7. 其他技術性資訊

- 惡意活動偵測紀錄
- 資安事件單
- 關聯事件單
- 疑似工及探測紀錄
- 關聯分析結果
- 漏洞資訊
- 攻擊手法
- 惡意程式
- 中繼站資訊
- 受害者資訊
- 惡意IP/DN
- 惡意郵件來源
- 中繼站黑名單阻擋統計
- 惡意程式分析報告
- 惡意活動趨勢分析
- 攻擊應變措施
- 資安趨勢報告
- 領域監控分析報告

資通安全認知與訓練

各責任等級應辦事項(制度面)

責任等級		資通系統分級及防護基準	資訊安全管理系統之導入CNS27001國際標準及通過公正第三方之驗證	專責人員	內部資通安全稽核	業務持續運作演練	資安治理成熟度評估
A	公務機關	1年內皆完成	• 2年內導入 • 3年內完成驗證	4名	2次/年	1次/年	1次/年
	特定非公務機關	1年內皆完成	• 2年內導入 • 3年內完成驗證	4名	2次/年	1次/年	--
B	公務機關	1年內皆完成	• 2年內導入 • 3年內完成驗證	2名	1次/年	1次/2年	1次/年
	特定非公務機關	1年內皆完成	• 2年內導入 • 3年內完成驗證	2名	1次/年	1次/2年	--
C	公務機關	• 1年內資通分級 • 2年內防護基準	• 2年內導入	1名	1次/2年	1次/2年	--
	特定非公務機關	• 1年內資通分級 • 2年內防護基準	• 2年內導入	1名	1次/2年	1次/2年	--

各責任等級應辦事項(技術面)

責任等級		安全性檢測		資通安全健診	資通安全監控管理機制	政府組態基準	資通安全防護					
		網站安全弱點檢測	系統滲透測試				防毒軟體	防火牆	郵件過濾	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦措施
A	公務機關	2次/年	1次/年	1次/年	○	○	○	○	○	○	○	○
	特定非公務機關	2次/年	1次/年	1次/年	○	○	○	○	○	○	○	○
B	公務機關	1次/年	1次/2年	1次/2年	○	○	○	○	○	○	○	--
	特定非公務機關	1次/年	1次/2年	1次/2年	○	--	○	○	○	○	○	--
C	公務機關	1次/2年	1次/2年	1次/2年	--	--	○	○	○	--	--	--
	特定非公務機關	1次/2年	1次/2年	1次/2年	--	--	○	○	○	--	--	--
D		--	--	--	--	--	○	○	○	--	--	--

各責任等級應辦事項(認知與訓練面)

責任等級		資通安全教育訓練		資通安全專業證照及職能訓練證書	
		資通安全及資訊人員(每人每年)	一般使用者與主管(每人每年)	資通安全專業證照(張)	資通安全職能訓練證書
A	公務機關	12小時 (4名)	3小時	4	4
	特定非公務機關	12小時(4名)	3小時	4	--
B	公務機關	12小時(2名)	3小時	2	2
	特定非公務機關	12小時(2名)	3小時	2	--
C	公務機關	12小時(1名)	3小時	1	1
	特定非公務機關	12小時(1名)	3小時	1	--
D		--	3小時	--	--

委外管理注意事項

委外單位資格

- 具備完善資通安全管理措施或通過協力廠商驗證
- 應配置之資安專業人員(數量、資格、證照、經驗)
- 得否複委託，及進行複委託應注之事項
- 涉及國家機密者，相關執行人員應接受適任性查核

委外作業管理

- 客製化開發者，應提供安全性檢測證明
- 非自行開發者應標示內容與其來源及提供授權證明
- 知悉資通安全事件時，應立即通知委託機關及採行之補救措施
- 委託結束後，應確認資料之返還或刪除
- 其他應採取資通安全相關維護措施
- 委託機關應稽核或適當方式確認執行情形

改善報告

稽核改善報告

- 缺失或待改善之項目與內容
- 發生原因
- 所採取管理、技術、人力或資源等層面之措施
- 預定完成時程及執行進度之追蹤

事件調查處理改善報告

- 事件發生、完成損害控制或復原作業之時間
- 損害控制及復原作業之歷程
- 事件調查及處理作業之歷程
- 防範再次發生所採取之管理、技術、人力或資源等層面之措施
- 預定完成時程及成效追蹤機制

THANKS FOR YOUR COOPERATION