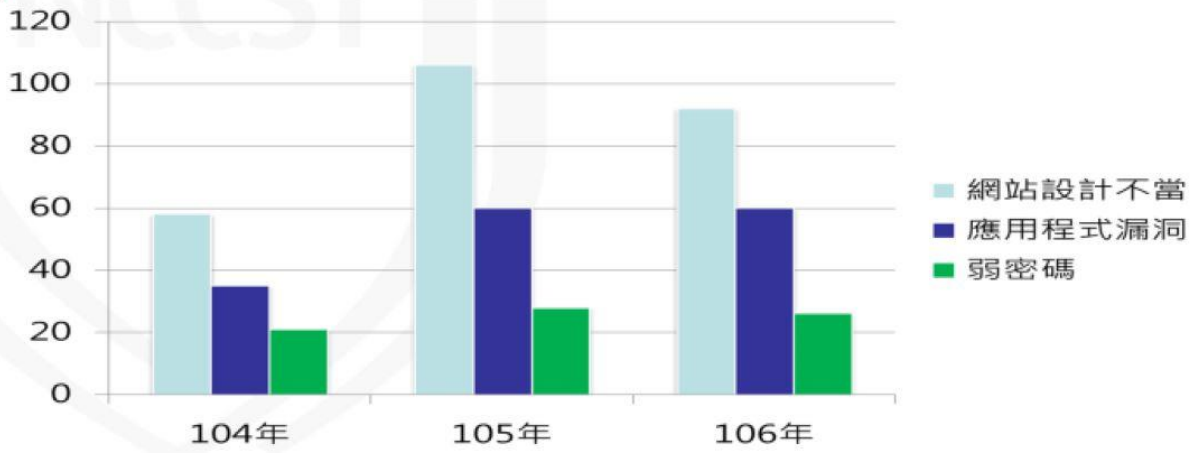
資安法上路實務，各單位準備好了嗎??

課程大綱

- 資通安全管理法
- 資通安全管理法規範重點
- 資安治理成熟度自我評審之流程重點說明
- 資安法三部曲
  - 第一部資通安全責任等級分級
  - 第二部資通安全維護計畫
  - 第三部資安治理成熟度

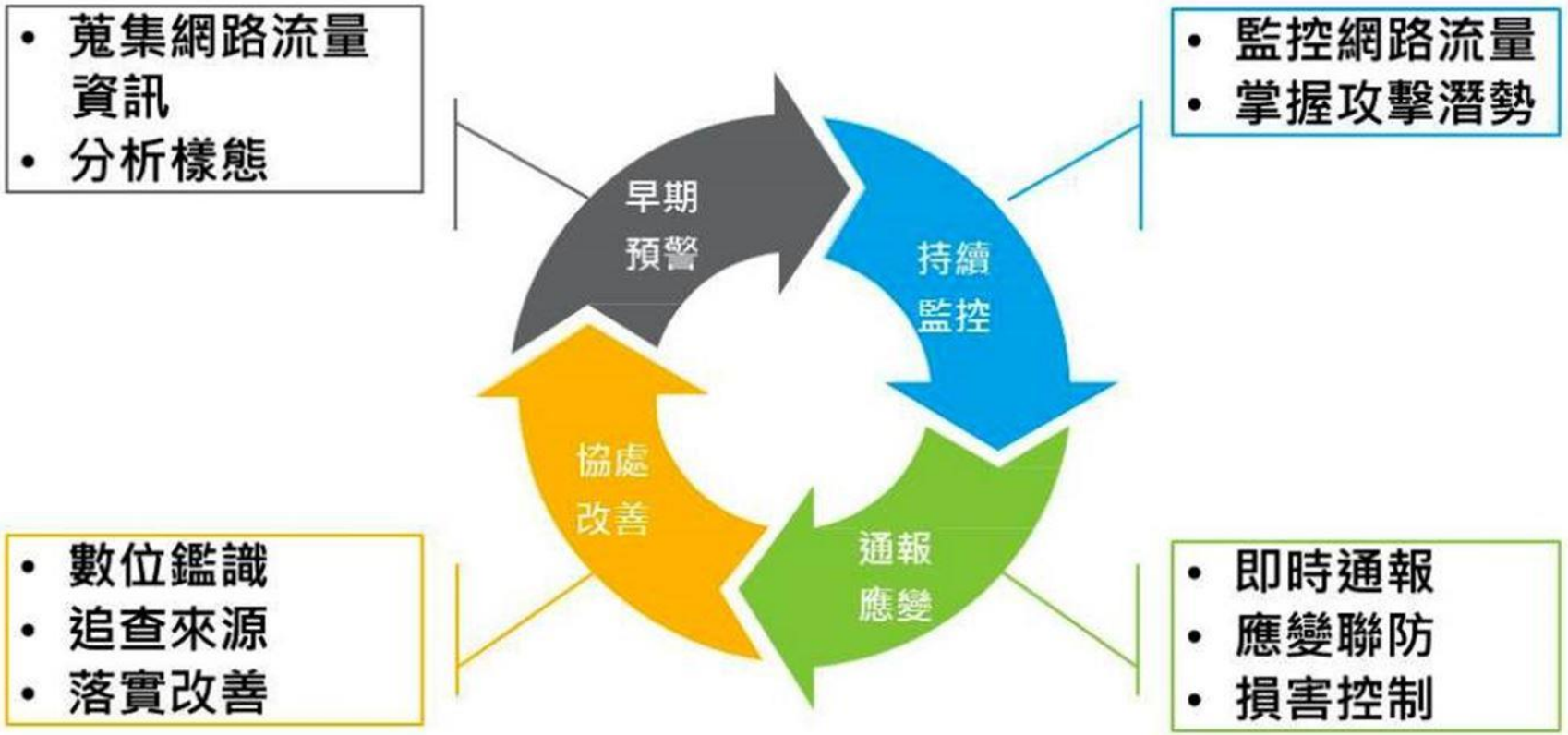
前言

- 106年接獲371件政府機關資安事件通報，以**網頁攻擊事件**類型為主，占40.21%
- 近三年資安事件發生原因，皆為網站設計不當、應用程式漏洞及弱密碼，部分受害設備轉為IoT設備
- 多數資安事件因未保留完整紀錄檔，導致無法確認事件發生原因

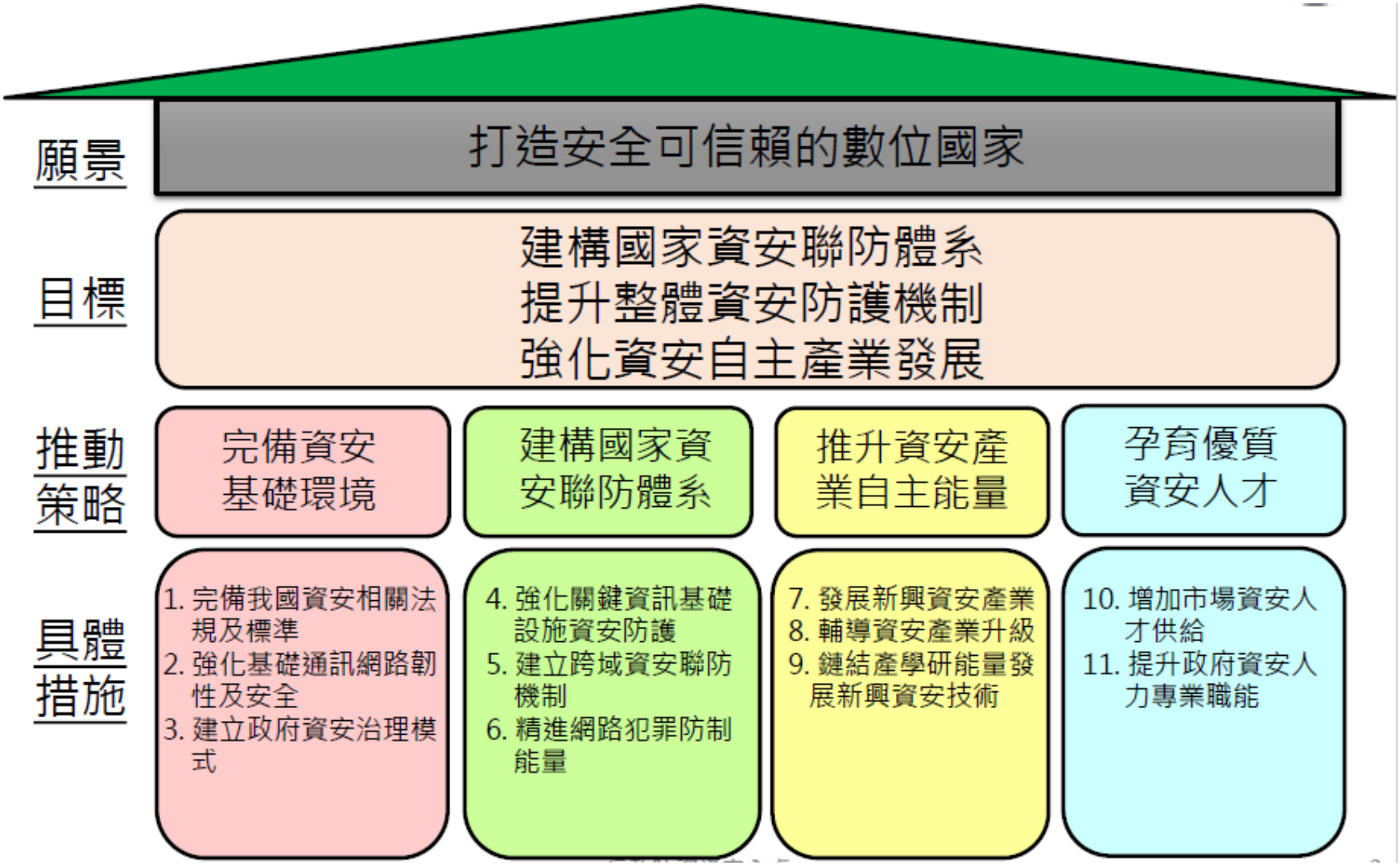


各國陸續將資通安全管理法立法

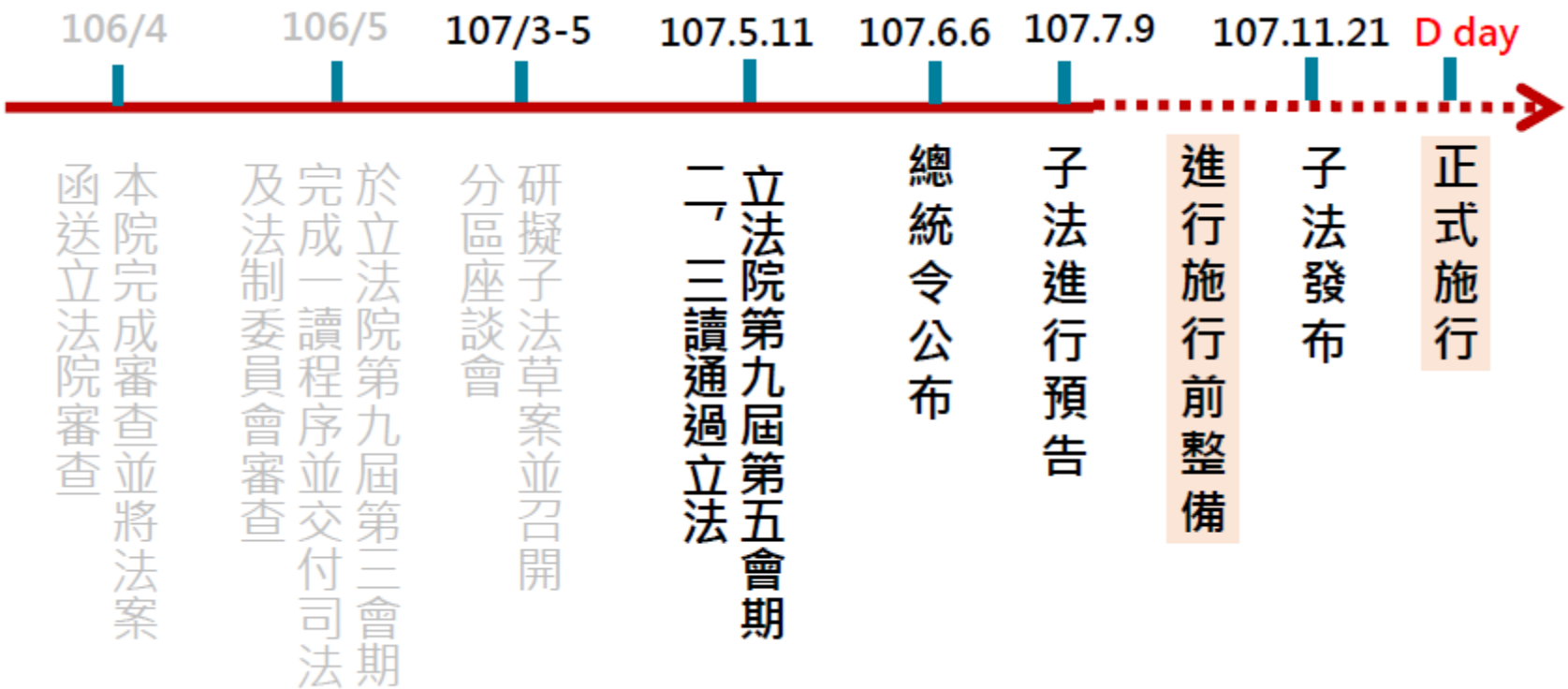
建立以風險管理為核心的防護架構



國家資通安全發展方案(106-109年)



資安法立法歷程



2019年1月1日 資安法管理正式施行

立法目的及適用對象

資通安全管理法

- 立法目的
  - 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
- 公告
  - 2018.5.11 立法院三讀通過
  - 2018.6.06 總統公告(總統華總一義字第10700060021號令)
- 實施
  - 行政院計畫該法之生效日期，將依照「公務機關」、「關鍵基礎設施提供者」、其他「特定非公務機關」之順序，分三波分別於該法通過後6個月、12個月、18個月後對其等生效
- 規範對象
  - 公務機關-(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
  - 八大關鍵基礎設施領域除政府機關以外，尚包含能源、水資源、通訊傳播、交通、金融、高科技園區及緊急救援與醫療

資安法結構

- 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

- **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**

- **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

- **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**

- **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
- 罰則

➢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。

➢規範對象

以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

公務機關

- 中央與地方機關(構)
- 公法人

特定非公務機關

- 關鍵基礎設施提供者 (如台電)
- 公營事業 (如台糖)
- 政府捐助之財團法人(如工研院)

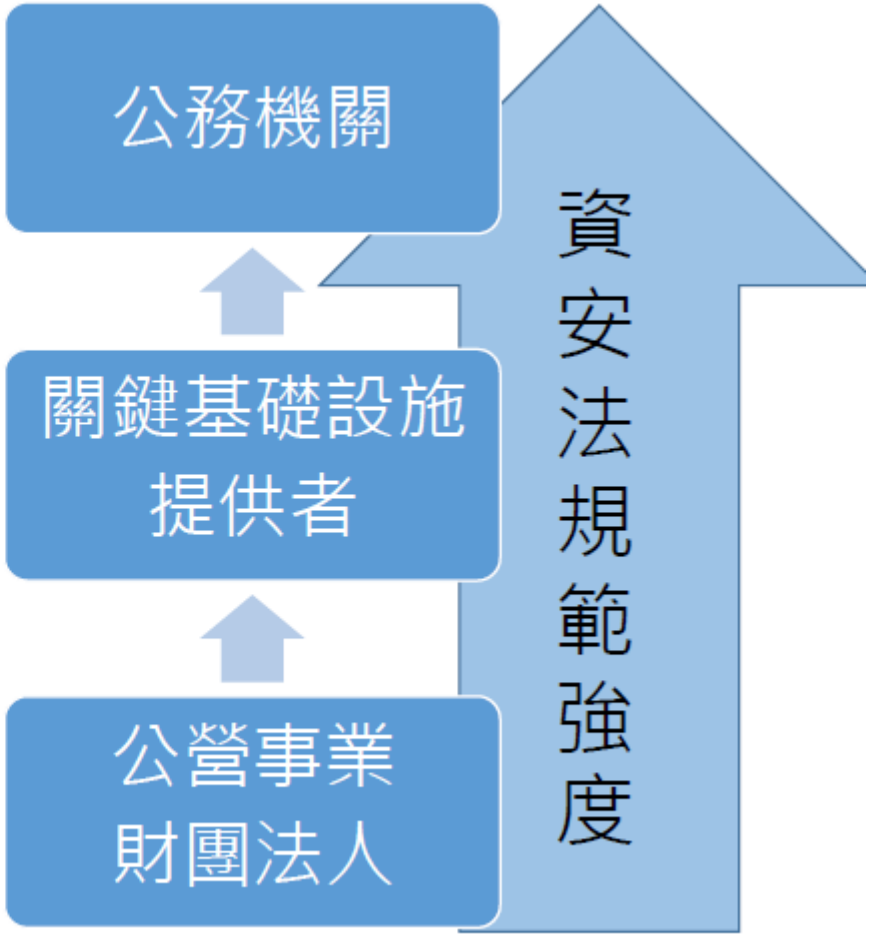
*資安管理法第3條第5款
公務機關：指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。

*資安管理法施行細則第2條
所稱軍事機關，指國防部及其所屬機關(構)、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款、第二項規定之機關。

關鍵基礎設施(CI)

本法規範適用先後

- 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



資通安全管理法之結構

立法目的與名詞定義

§1、§3

主管機關應辦事項

§2、§4~§9

公務機關資通安全管理

§10~§15

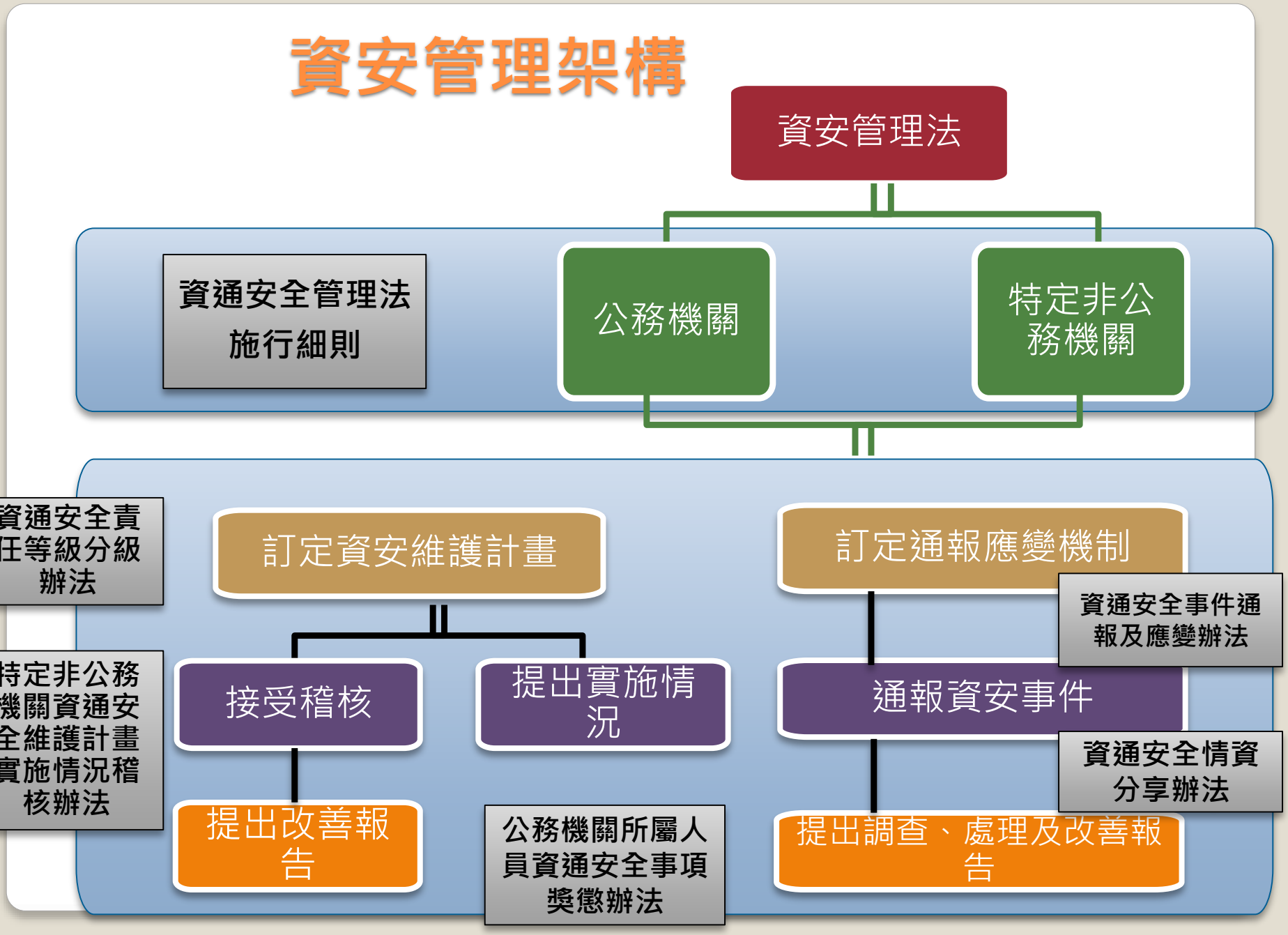
特定非公務機關資通安全管理

§16~§18

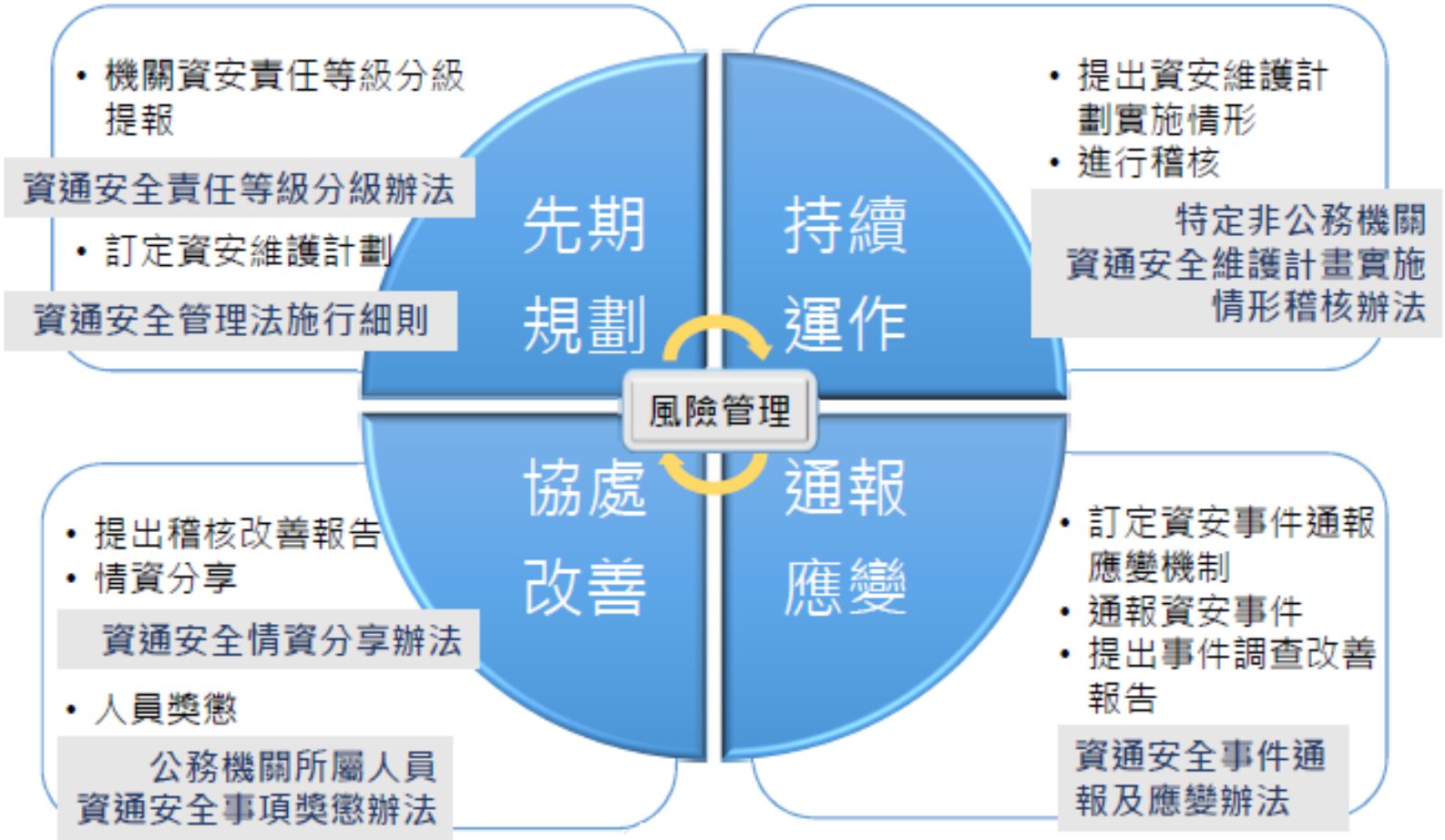
罰則

§19~§21

資安管理架構


資安管理法
資通安全管理法施行細則
公務機關
特定非公務機關
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
特定非公務機關資通安全維護計畫實施情況稽核辦法
接受稽核
提出實施情況
通報資安事件
資通安全情資分享辦法
提出改善報告
公務機關所屬人員資通安全事項獎懲辦法
提出調查、處理及改善報告

以風險管理為核心的資安防護



資通安全管理法之子法

- 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況稽核辦法
- 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

公務機關之資通安全管理

✓ 應訂定資通安全維護計畫§9
✓ 應訂定通報及應變機制§13 I

行政院

- 擘劃並推動國家資通安全政策
- 資通安全科技發展
- 國際交流合作及資通安全整體防護
- 定期公布國家資安情勢報告及資通安全發展方案

- 應提出年度資通安全維護計畫之實施情形§11
- 應提出改善報告§12 II
- 應通報資通安全事件§13 II
- 應提出資通安全事件之調查、處理及改善報告§13 III

上級或監督機關 ⇄ 下級或受監督機關

- 應稽核資通安全維護計畫實施情形§12 I

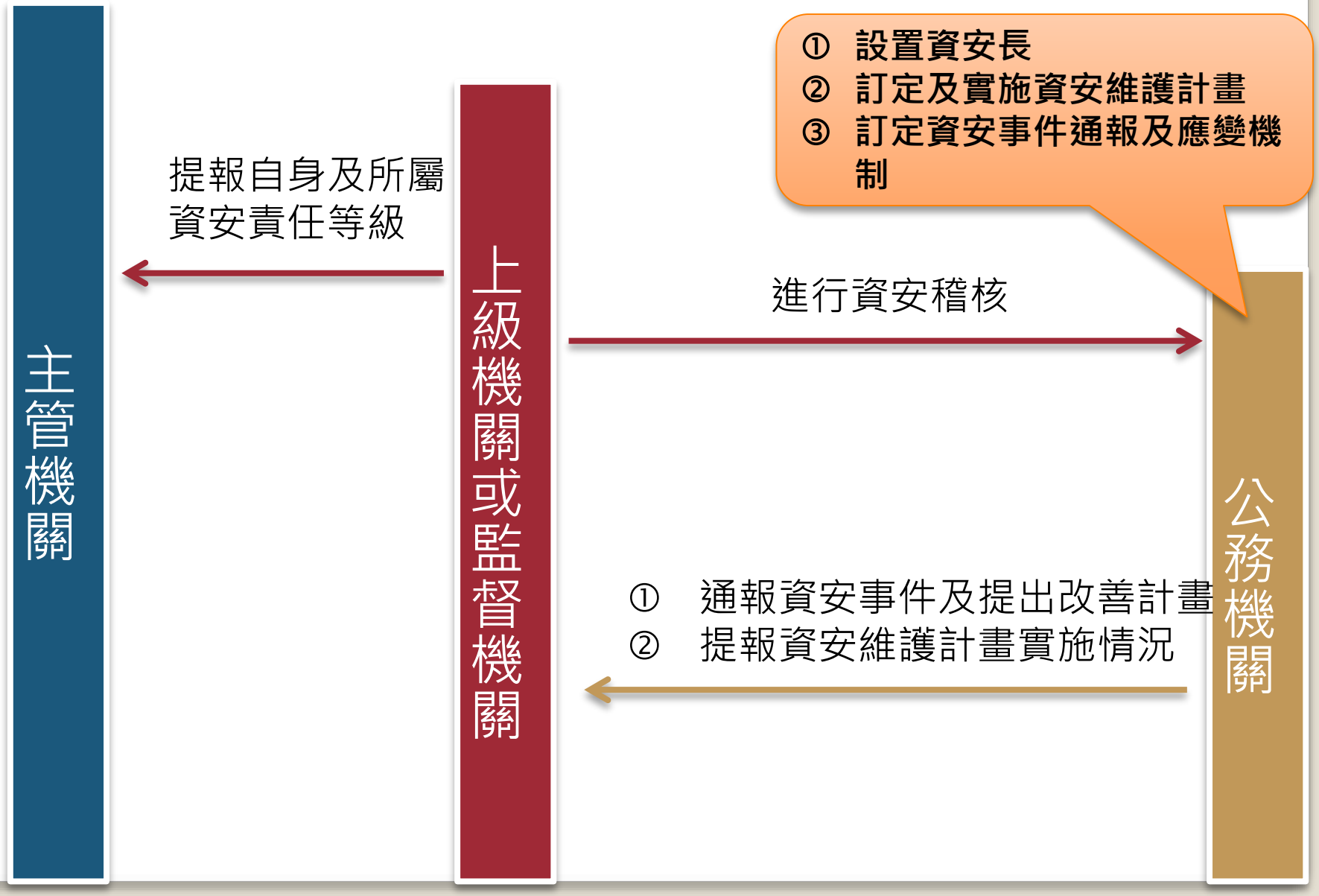
總統府、立法院、司法院、考試院、監察院、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會

設置資通安全長§10

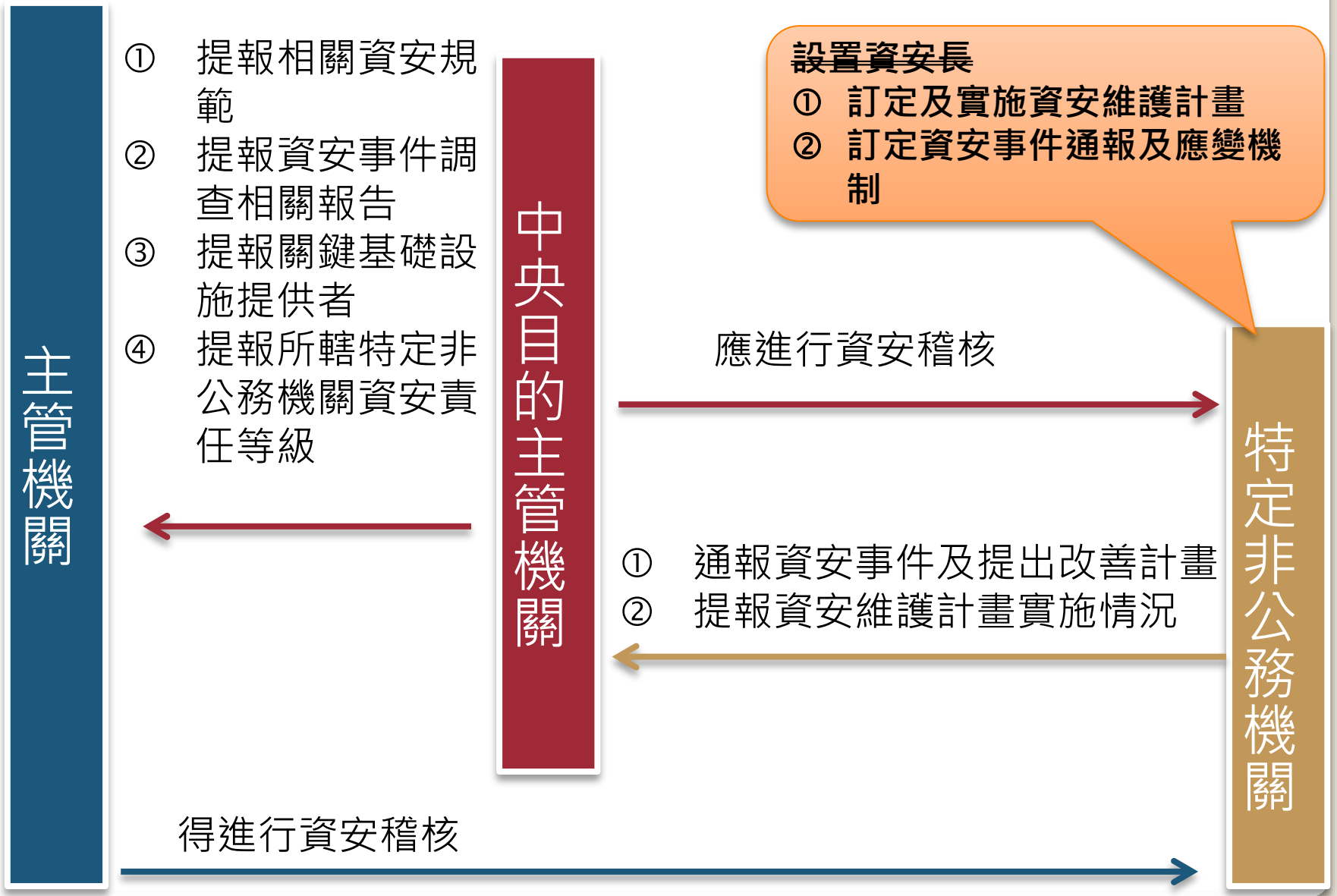
訂定

- ✓資安管理法施行細則§22
- ✓資安責任等級分級辦法§6
- ✓資安事件通報及應變辦法§13、17
- ✓維護計畫實施情形稽核辦法§6、12
- ✓資安情資分享辦法§7

法遵要求 - 公務機關


主管機關
上級機關或監督機關
公務機關
① 設置資安長
② 訂定及實施資安維護計畫
③ 訂定資安事件通報及應變機制
提報自身及所屬資安責任等級
進行資安稽核
① 通報資安事件及提出改善計畫
② 提報資安維護計畫實施情況

法遵要求 - 特定非公務機關



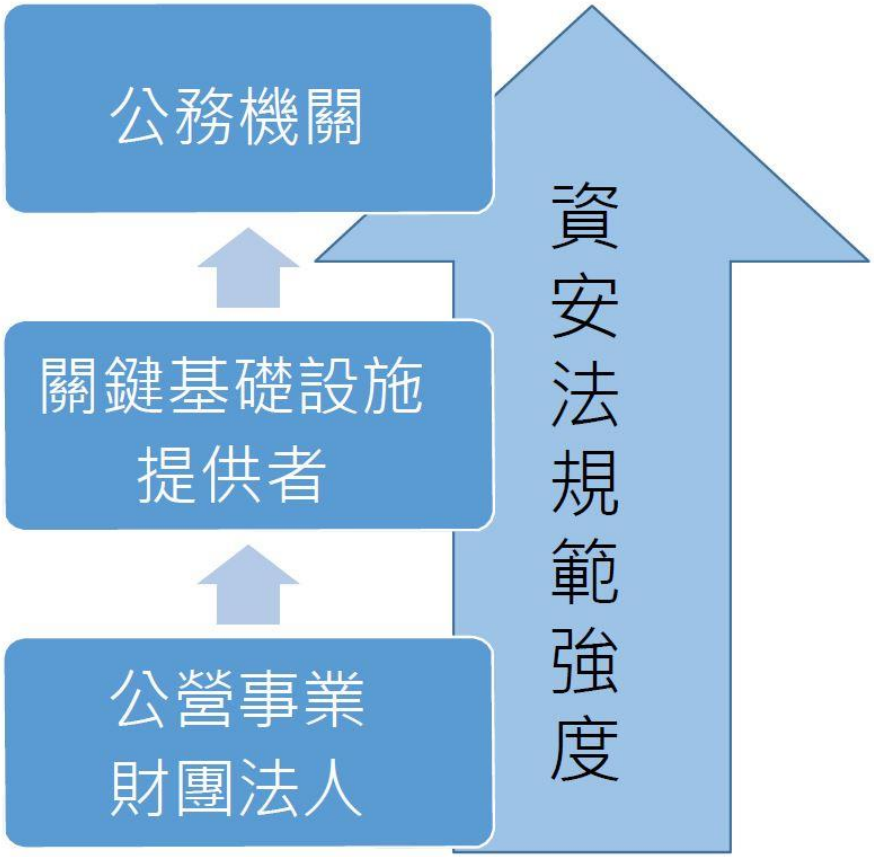
罰則

- 特定非公務機關如違反資通安全管理法所要求相關義務，由中央目的事業主管機關令限期改正。
- 屆期未改正者，按次處新臺幣10萬元以上100萬元以下罰鍰。

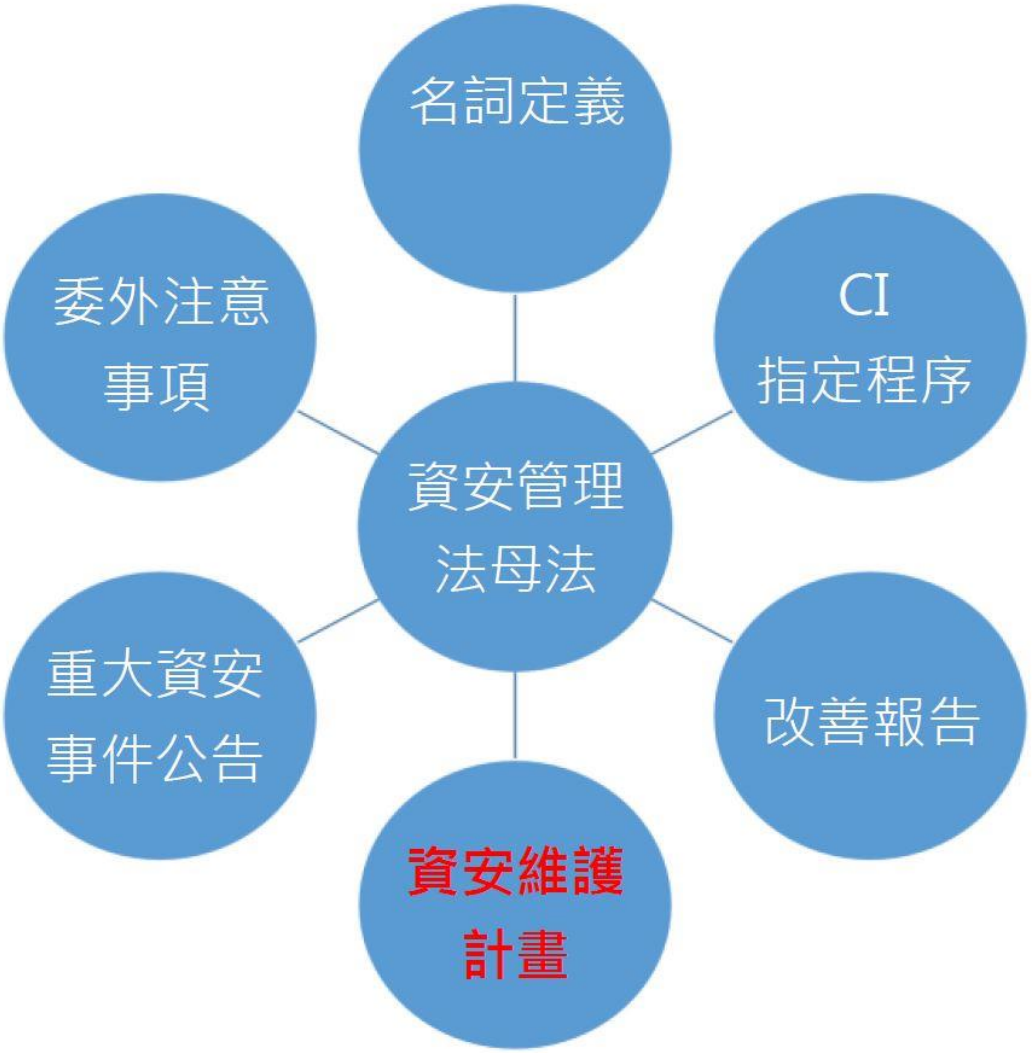
- 特定非公務機關未依規定通報資通安全事件者，由中央目的事業主管機關處新臺幣30萬元以上500萬元以下罰鍰，並令限期改正。
- 屆期未改正者，按次處罰之。

本法規範適用強度

- 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

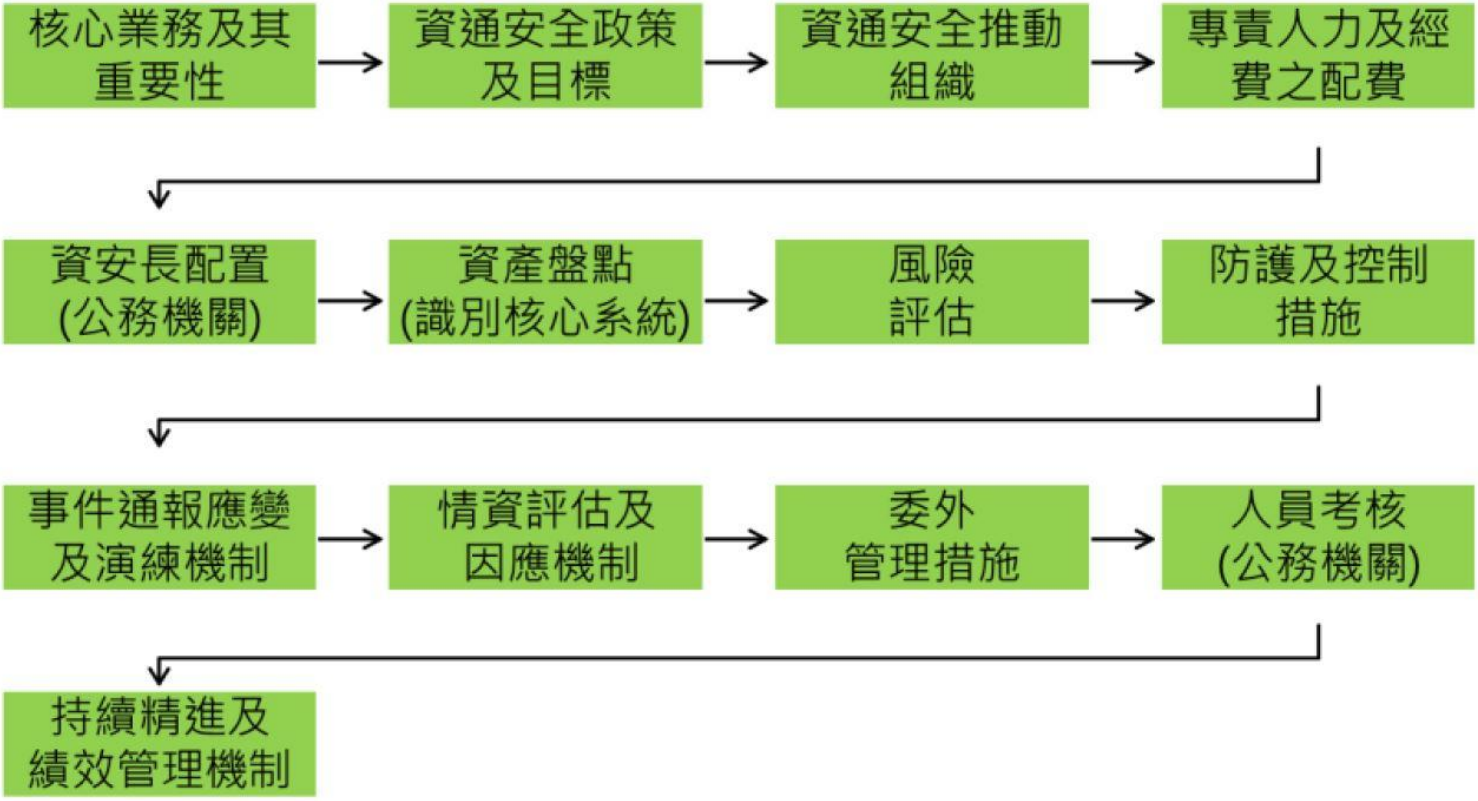


資通安全管理法施行細則



資通安全維護計畫內容

- **細則§6**　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。

資通系統建置、服務委外辦理注意事項

- 考量委外項目之性質、資通安全需求，選任適當之受託者，並監督其資通安全維護。
  - 資安法施行後, 不論是新開發或是增修，只要有委外就要適用。
  - 考量個案不同，受託者可自行使用第三方軟體進行安全性檢測。
  - 惟如該資通系統屬委託機關之核心資通系統，或委託案件金額在1,000萬元以上，委託機關應自行或另行委託第三方進行安全性檢測。

委外之前

- 受託者應具備完善之資通安全管理措施或通過第三方驗證
- 受託者應配置之資安專業人員(數量、資格、證照、經驗)
- 受託者得否複委託，及進行複委託應注之事項
- 受託業務涉及國家機密者，相關執行人員應接受適任性查核

委外之後

- 客製化開發者，應提供該資通系統之安全性檢測證明
- 非自行開發者，並應標示內容與其來源及提供授權證明。
- 受託者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，應確認受託者持有之資料之返還或刪除
- 受託者應採取之其他資通安全相關維護措施
- 委託機關應以稽核或適當方式確認受託者之執行情形

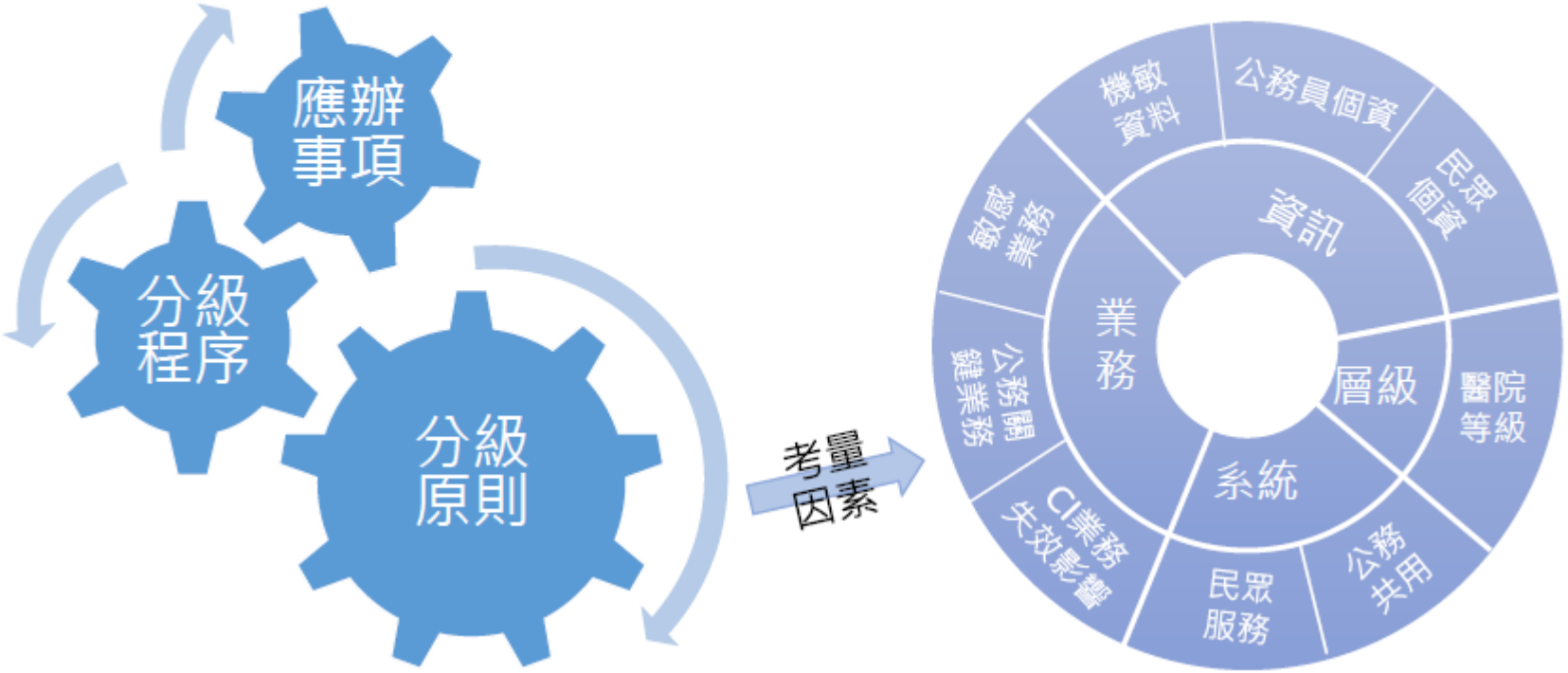
改善報告內容要求

- 稽核改善報告(§3)
  - 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

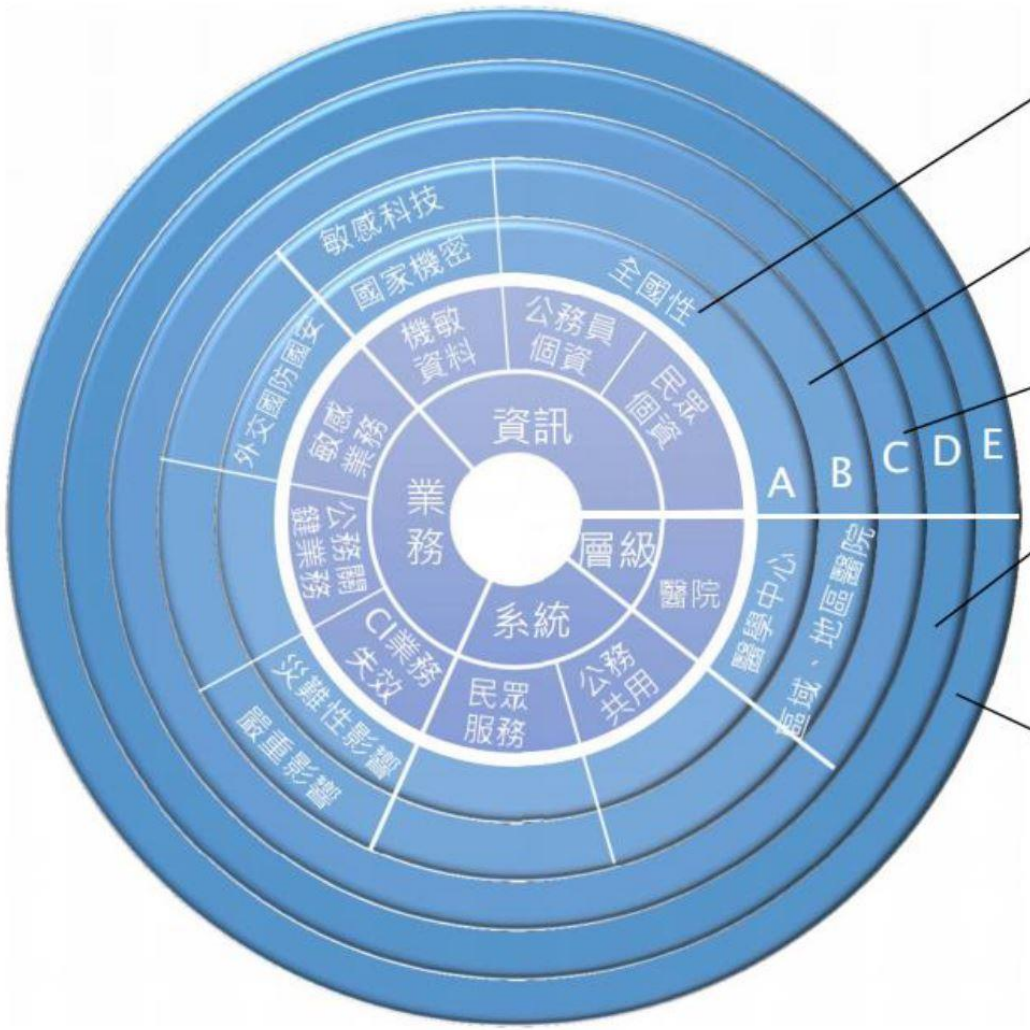
- 事件調查處理改善報告(§8)
  - 事件發生、完成損害控制或復原作業之時間
  - 事件影響之範圍及損害評估
  - 損害控制及復原作業之歷程、事件調查及處理作業之歷程
  - 事件根因分析
  - 防範再次發生所採取之管理、技術、人力或資源等層面之措施
  - 預定完成時程及成效追蹤機制

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。
- 後續依該責任等級辦理相對應之應辦事項



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

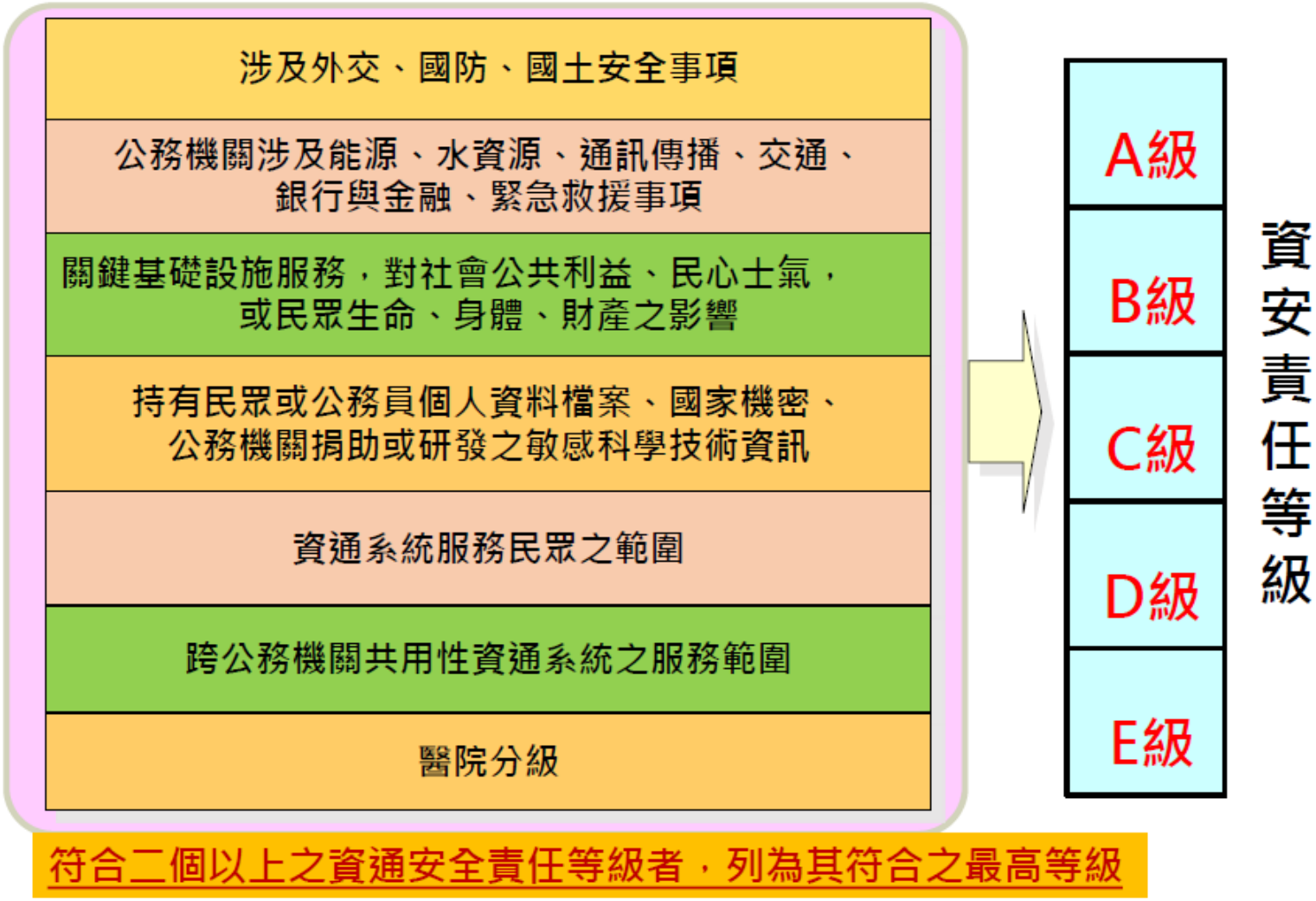
C級：維運自行或委外開發資通系統

D級：未維運自行或委外開發資通系統，惟仍自行辦理資通業務

E級：無自行辦理資通業務，或全部業務由其他機關兼辦或資訊代辦

§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

資安責任等級分級執行作業



應辦事項-管理面

辦理項目	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內	1年內	2年內
資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入資訊安全管理系統，並於三年內完成第三方驗證；並持續維持其驗證有效性	2年內	2年內	2年內
業務持續運作演練	全部核心資通系統	每年1次	每2年1次	每2年1次
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專責人員(一年內)		專職(責)4人	專職(責)2人	專職(責)1人
資安治理成熟度評估(公務機關)		每年1次	每年1次	

應辦事項-技術面

辦理項目	辦理內容	A	B	C
安全性檢測	全部核心資通系統網站安全弱點檢測	每年2次	每年1次	每2年1次
	全部核心資通系統系統滲透測試	每年1次	每2年1次	每2年1次
資通安全健診	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視	每年1次	每2年1次	每2年1次
資通安全威脅偵測管理機制	完成威脅偵測機制建置，並持續維運	1年內	1年內	
	依主管機關指定之方式提交監控管理資料(公務機關)	V	V	

資安健診

- 任何運作中的電腦環境都有可能受到攻擊。
- 成功的攻擊通常是經過不斷失敗的攻擊之後發生。
- 越早發現攻擊就越容易遏制損害的發生。
- 資安健診與入侵偵測
  - 誰該為攻擊負責
  - 可以辨識攻擊模式。
  - 找出未知的安全性設定問題
  - 協助判斷哪些網路資源是漏洞所在。

如何健診環境以掌握發現攻擊的最佳契機

資安健診項目

1. 網路架構檢視
   - 依據貴單位提供之網路架構圖，從網路架構設計、設備位置部署及防護程度等面向，分析網路架構是否有須加強。

2. 有線網路惡意活動檢視
   - 藉由封包監聽及網路設備紀錄檔，分析貴單位網路流量是否符合異常、惡意之連線行為。

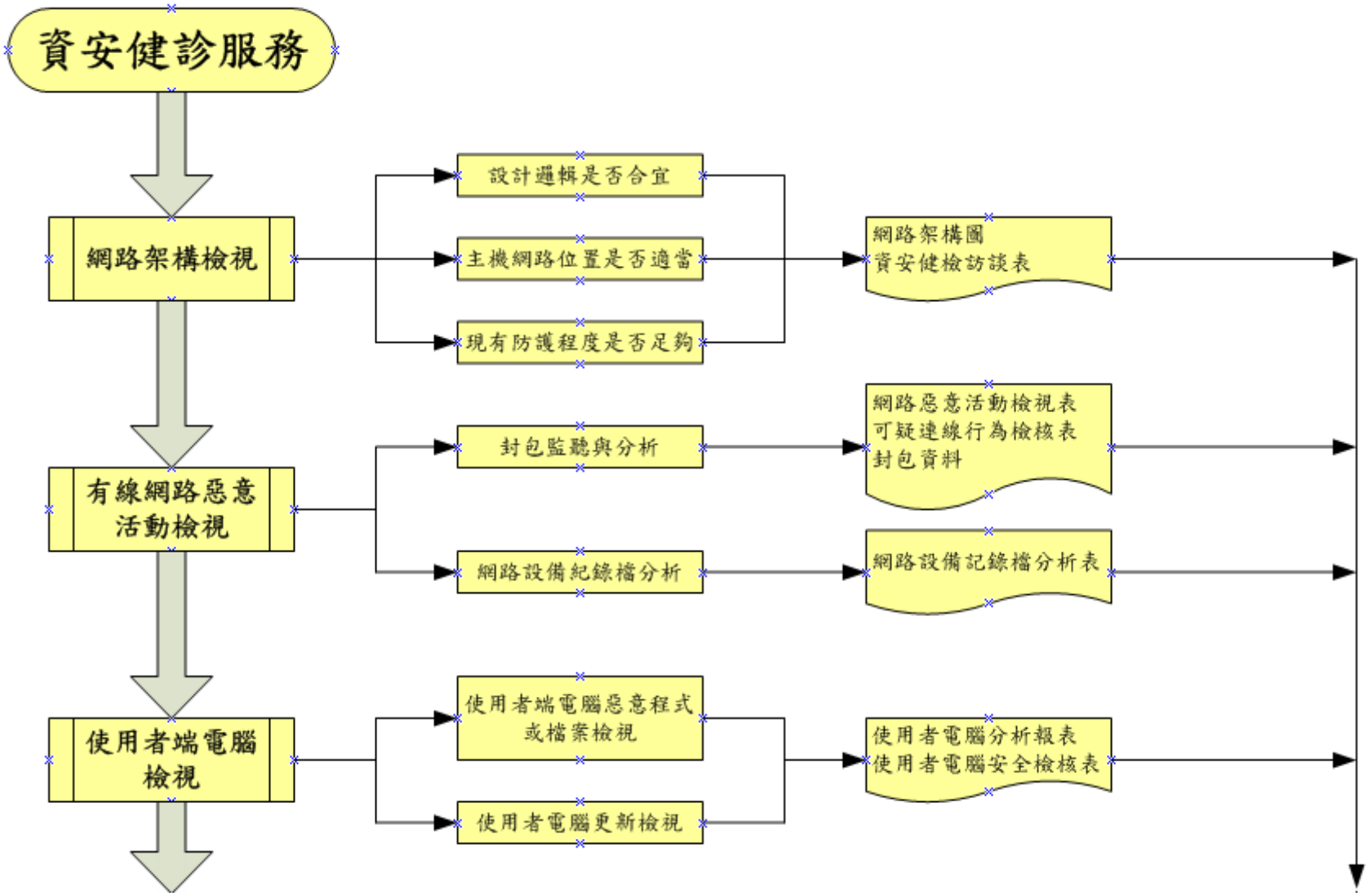
3. 使用者端電腦檢視
   - 檢視使用者端電腦是否存在惡意程式、異常之活動中連線。
   - 作業系統、Office 應用程式、防毒軟體、Adobe Acrobat及Adobe flash player 應用程式更新檢視。
   - 政府組態基準

資安健診項目

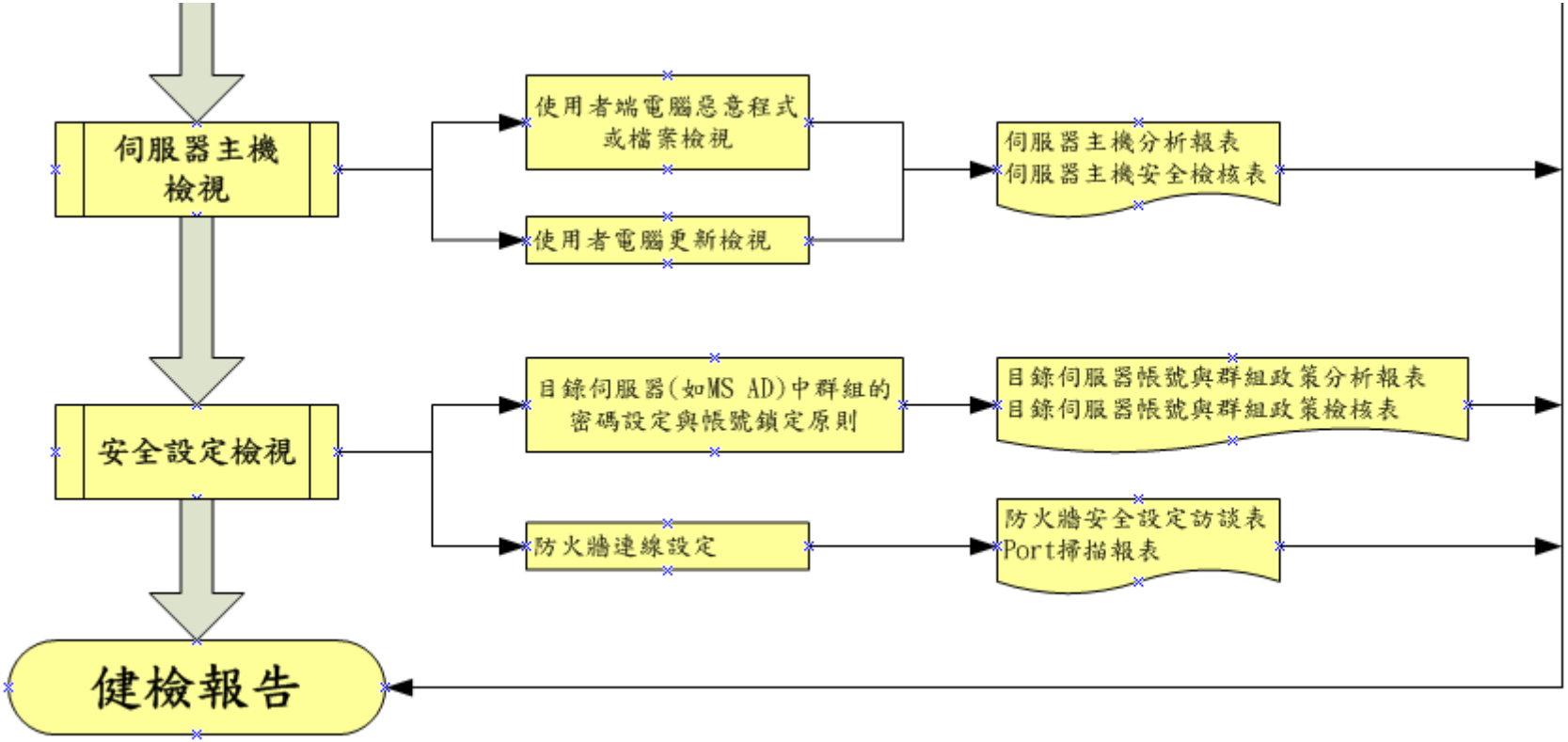
4. 伺服器主機檢視
   - 檢視伺服器主機是否存在惡意程式、異常之活動中連線。
   - 作業系統、Office 應用程式、防毒軟體、Adobe Acrobat及Adobe flash player 應用程式更新檢視。

5. 安全設定檢視
   - 檢視目錄伺服器之密碼設定及帳號鎖定原則的安全性等級是否足夠。
   - 檢視防火牆管理帳號及規則設定是否適宜。

執行方式 - 資安健診


資安健診服務
網路架構檢視
設計邏輯是否合宜
主機網路位置是否適當
現有防護程度是否足夠
網路架構圖
資安健檢訪談表
有線網路惡意活動檢視
封包監聽與分析
網路設備紀錄檔分析
網路惡意活動檢視表
可疑連線行為檢核表
封包資料
網路設備記錄檔分析表
使用者端電腦檢視
使用者端電腦惡意程式或檔案檢視
使用者電腦更新檢視
使用者電腦分析報表
使用者電腦安全檢核表

執行方式 - 資安健診 (續)

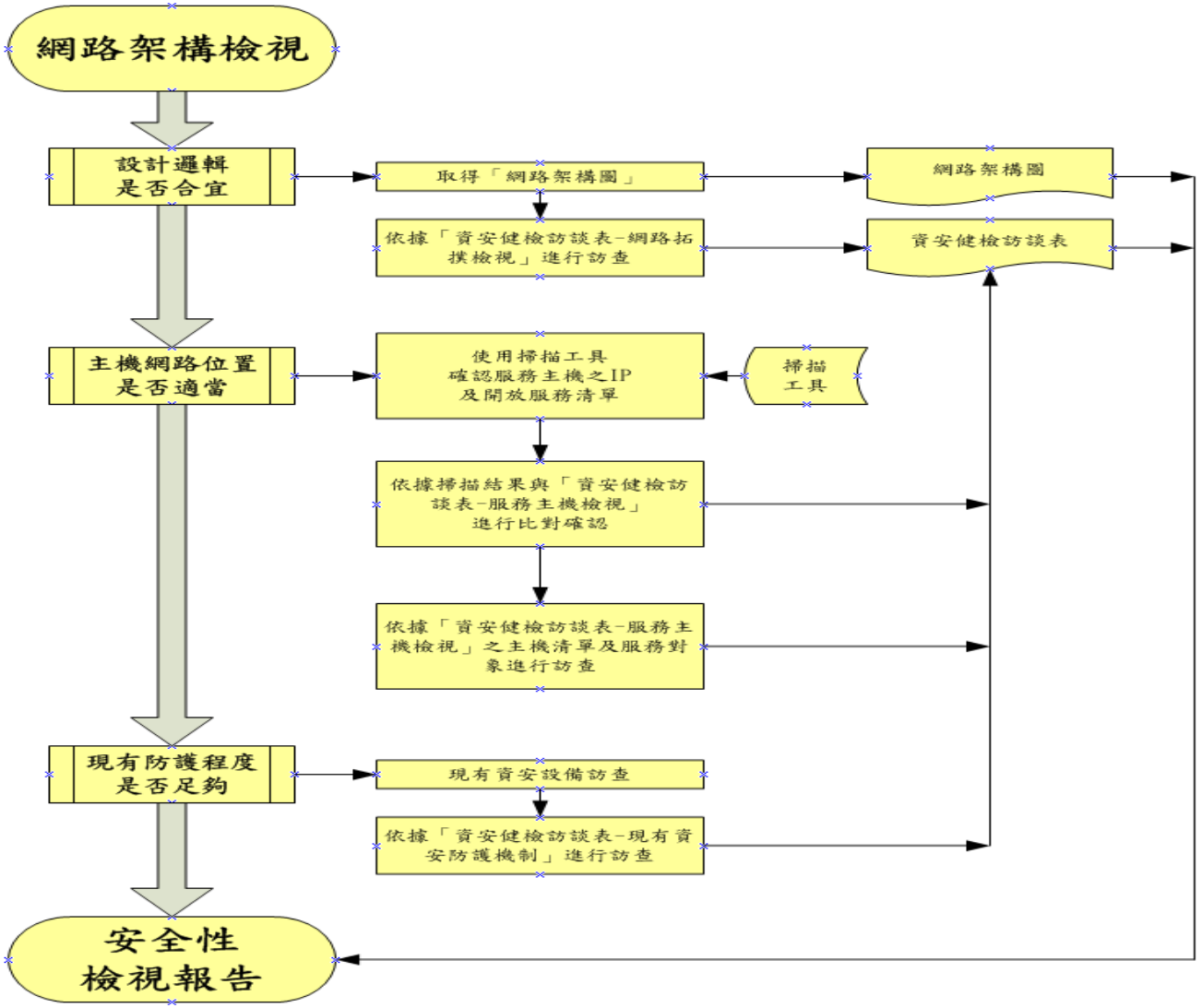

伺服器主機檢視
使用者端電腦惡意程式或檔案檢視
使用者電腦更新檢視
伺服器主機分析報表
伺服器主機安全檢核表
安全設定檢視
目錄伺服器(如MS AD)中群組的密碼設定與帳號鎖定原則
目錄伺服器帳號與群組政策分析報表
目錄伺服器帳號與群組政策檢核表
防火牆連線設定
防火牆安全設定訪談表
Port掃描報表
健檢報告

(一)資訊架構檢視

1. 檢視網路架構之配置、資訊設備安全管理規則之妥適性等，以評估可能之風險，採取必要因應措施。
2. 檢視單點故障最大衝擊與風險承擔能力。
3. 檢視對於持續營運所採取相關措施之妥適性。

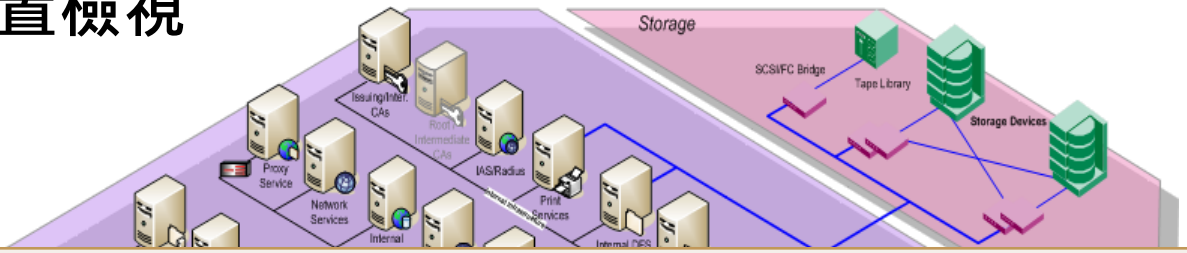
提供網路架構圖，並安排相關人員接受訪談。

(一)執行方式 - 資安健診（網路架構檢視）



(一)資訊架構檢視

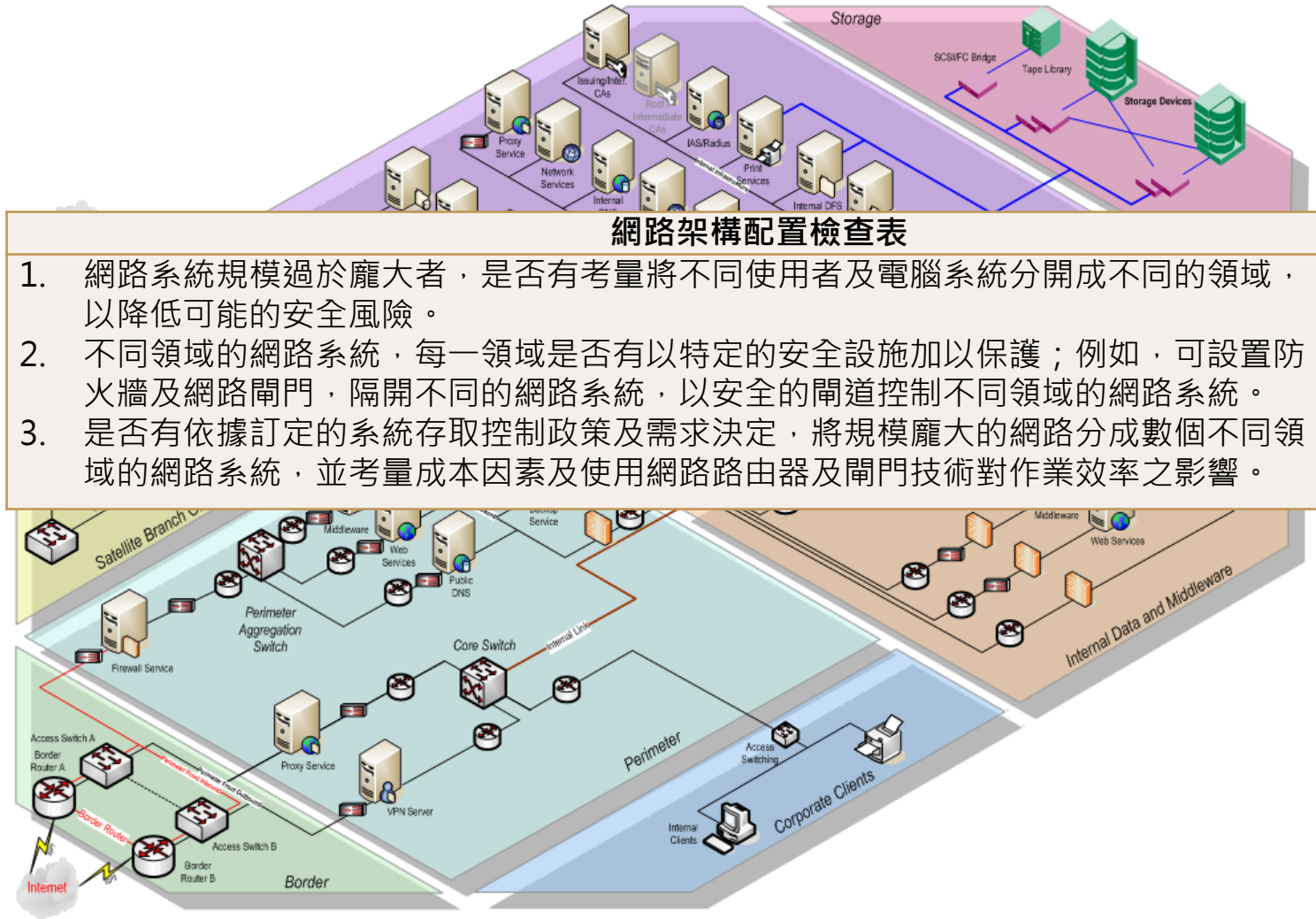
1.網路架構配置檢視



網路架構設計邏輯是否合宜		
1.	是否於內、外網路連接的邊界處，架設防火牆、IPS等網路安全控管機制，以確保網路存取與資料傳輸的安全。	□是 □否
2.	對於跨組織之電腦網路系統，是否有架設防火牆與通訊保密機制以加強網路安全。	□是 □否
3.	如利用公眾網路傳送敏感性資訊，是否有採取安全保護措施，以保護資料在公共網路傳輸的完整性及機密性。	□是 □否
4.	為維持機關網路的持續正常運作，各重要網路設備是否有備援系統。	□是 □否
5.	是否有針對網路硬體設備加裝不斷電系統，以防止不正常的斷電狀況。	□是 □否
6.	為確保內部網路與外界的服務持續暢通，內部網路與外界網路的連接，是否有一個以上的替代路徑。	□是 □否
7.	從使用者端末機連接電腦系統之線路，是否有適當加以控制（例如:建立強制性的通道），以減少未經授權存取系統或電腦設施之風險。	□是 □否 □是 □否
8.	是否有建立強制性的通道，防止未被授權的使用者從不同的管道進入電腦系統。	
9.	開放機關以外的使用者從公眾網路，或從機關網路以外的網路與本機關連線作業，是否有建立遠端使用者身分鑑別機制，以降低未經授權存取系統的風險。	□是 □否
10.	分享式的網路系統（尤其是跨機關的網路系統），是否有建立網路路由的控制，以確保電腦連線作業及資訊流動，不會影響應用系統的存取政策。	□是 □否

(一)資訊架構檢視

2.單點故障衝擊及風險檢視



網路架構配置檢查表	
1. 網路系統規模過於龐大者，是否有考量將不同使用者及電腦系統分開成不同的領域，以降低可能的安全風險。	□是 □否
2. 不同領域的網路系統，每一領域是否有以特定的安全設施加以保護；例如，可設置防火牆及網路閘門，隔開不同的網路系統，以安全的閘道控制不同領域的網路系統。	□是 □否
3. 是否有依據訂定的系統存取控制政策及需求決定，將規模龐大的網路分成數個不同領域的網路系統，並考量成本因素及使用網路路由器及閘門技術對作業效率之影響。	□是 □否

作業名稱 / 等級	資訊系統分類分級	ISMS 推動作業	資安專責人力	稽核方式	業務持續運作演練	防護縱深	監控管理	安全性檢測	資安教育訓練(一般主管、資訊人員/資安人員、一般使用者	專業證照
A 級	1.完成資訊系統分級(104 年底前)。 2.完成資訊系統資安防護基準要求(105 年底前)。	1.全部核心資訊系統完成 ISMS 導入(105 年底前)。 2.全部核心資訊系統通過第三方驗證(106 年底前)。	指派資安專責人力 2 人。	每年至少 2 次內稽。	每年至少辦理 1 次核心資訊系統持續運作演練。	1.防毒、防火牆、郵件過濾裝置。 2.IDS/IPS、Web 應用程式防火牆。 3.APT 攻擊防禦。	SOC 監控(104 年底前)。	1.每年至少辦理 2 次網站安全弱點檢測。 2.每年至少辦理 1 次系統滲透測試。 3.每年至少辦理 1 次資安健診。	1.每年資安人員(資訊人員)至少 2 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練。 2.每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過課程評量。	每年維持至少 2 張國際資安專業證照與 2 張資安職能訓練證書之有效性。
B 級	1.完成資訊系統分級(104 年底前)。 2.完成資訊系統資安防護基準要求(105 年底前)。	1.至少 2 項核心資訊系統完成 ISMS 導入(106 年底前)。 2.至少 2 項核心資訊系統通過第三方驗	指派資安專責人力 1 人。	每年至少 1 次內稽。	每 2 年至少辦理 1 次核心資訊系統持續運作演練。	1.防毒、防火牆、郵件過濾裝置。 2. IDS/IPS。 3. Web 應用程式防火牆(機關具有對外服務之核心資訊系統)。	SOC 監控(105 年底前)。	1.每年至少辦理 1 次網站安全弱點檢測。 2.每 2 年至少辦理 1 次系統滲透測試。 3.每 2 年至少辦理 1 次	1.每年資安人員(資訊人員)至少 1 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練。 2.每年一般使用者與主管至少須接受 3 小時	每年維持至少 1 張國際資安專業證照與 1 張資安職能訓練證書之有效性。

作業名稱 等級	資訊系統分類分級	ISMS 推動作業	資安專責人力	稽核方式	業務持續運作演練	防護縱深	監控管理	安全性檢測	資安教育訓練(一般主管、資訊人員/資安人員、一般使用者	專業證照
		證(107 年底前)						資安健診	資安專業課程並通過課程評量	
C 級	依各主管機關規定	自行成立推動小組規劃作業	依各主管機關規定	依各主管機關規定	依各主管機關規定	1.防毒 2.防火牆 3.郵件過濾裝置(機關具有郵件伺服器)	依各主管機關規定	依各主管機關規定	1.依各主管機關規定資安人員(資訊人員)資安專業課程訓練或資安職能訓練要求 2.每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過課程評量	依各主管機關規定

(一)網路架構檢測檢核內容

項次	檢核內容	檢核結果	風險
1	網路系統架構區域 規劃網路區域，如伺服器區、資料庫區	未規劃網路區域	高
		未依規劃置放系統服務	中
2	網路區域間的存取 各區域間部署防火牆、配置相關存取控制	未配置網路區域間的存取	高
3	部署入侵偵測/防禦系統	未部署入侵偵測/防禦系統	中
4	部署系統本機安全機制 如HIDS、HIPS、本機防火牆	未部署系統本機安全機制	低
5	建立實體備援機制 從主機端至服務出口端經過的設備	重要系統未建立實體備援機制	中
6	建立服務備援機制 網域名稱服務、系統服務	重要服務未建立服務備援機制	中
7	限制內部對外連線	未限制內部對外部連線	中
8	限制外部對內連線	未限制外部對內部連線	高
9	限制服務區域連線	未限制服務區域連線	高

(一)網路架構檢測檢核內容

項次	檢核內容	檢核結果	風險
10	應不包含Permit All/Any於任一個規則	包含Permit All/Any	高
11	應定義Deny All/Any於最後一個規則	未定義Deny All/Any	中
12	限制非加密資料傳輸協定	外部資料交換未使用加密資料傳輸	中
		內部資料交換未使用加密資料傳輸	建議
13	第三方連線存取控制	未配置第三方連線存取控制	中
14	遠端連線存取控制	未配置遠端連線存取控制	高
15	網路設備存取認證	未配置網路設備存取認證	中
		使用本機認證，未使用中央認證系統	建議
16	網路設備存取控制	未配置網路設備存取控制	中
		已配置存取控制，但未生效	中

(一)網路架構檢測檢核內容

項次	檢核內容	檢核結果	風險
17	網路設備SNMP設定	配置可寫SNMP，使用預設通行碼	高
		配置唯讀SNMP，使用預設通行碼	中
		使用預設通行碼，但有配置存取控制	低
18	網路設備校時設定	未配置校時設定	中
		已配置校時設定，但未生效	中

(二)網路活動檢視

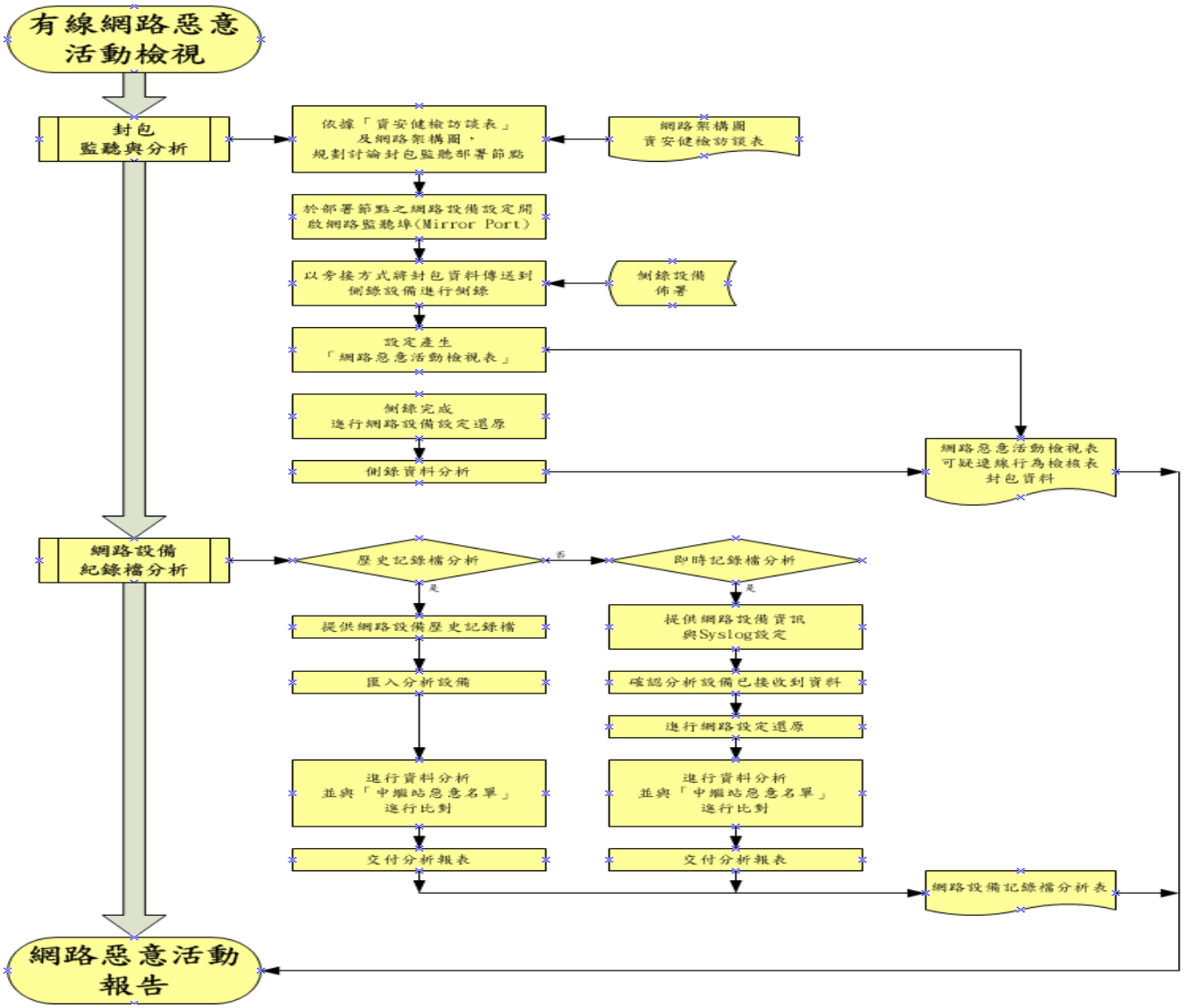
1. 檢視網路設備、伺服器之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。
2. 檢視資安設備(如：防火牆、入侵偵測系統、防毒軟體、資料外洩防護等)之監控紀錄，識別異常紀錄與確認警示機制。

(網路設備紀錄檔分析以1個月或100 Mbyte內的紀錄為原則)

3. 檢視網路封包是否存在異常連線或異常網域名稱解析伺服器(Domain Name System Server，DNS Server)查詢，並比對是否為已知惡意IP、中繼站或有符合網路惡意行為的特徵。

(封包側錄以至少6小時為原則，以觀察是否有異常連線)

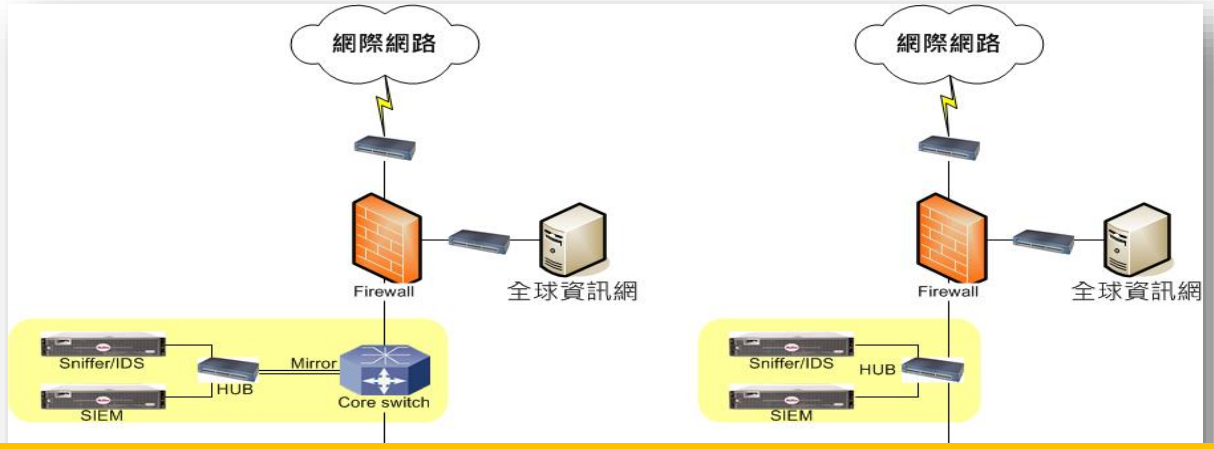
(二)執行方式 - 資安健診（有線網路惡意活動檢視）



(二)網路活動檢視

1.網路設備記錄檔分析

採用之技術方法	檢視是否有以下網路惡意活動
1. 以SIEM收集設備紀錄檔分析	✓ 異常連線或DNS 查詢。 ✓ 是否連線已知惡意IP、中繼站(C&C) ✓ 有符合惡意網路行為的特徵。 ✓ 分析過濾異常連線紀錄。

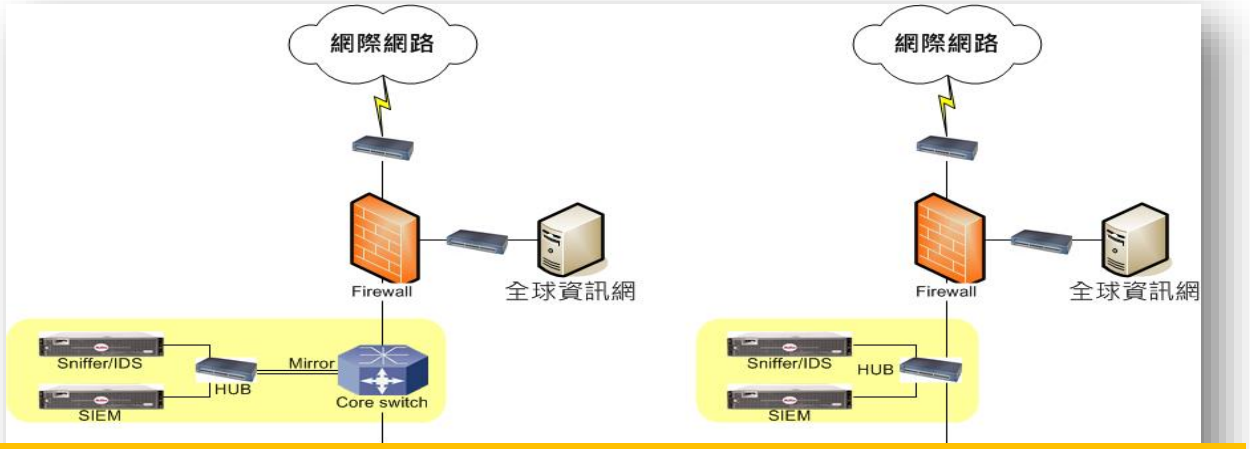


- 在現場收集或由客戶提供相關設備紀錄檔，在現場或帶回公司，透過分析系統工具進行紀錄檔之比對分析，分析結果會與受測機關進行確認以降低誤判，以檢視受測機關的網路環境，是否有符合可疑或異常網路活動之資安事件，並提出可能影響業務營運之潛在威脅。
- 可支援分析紀錄檔的設備廠牌類型以目前市場上之主流產品為主。

(二)網路活動檢視

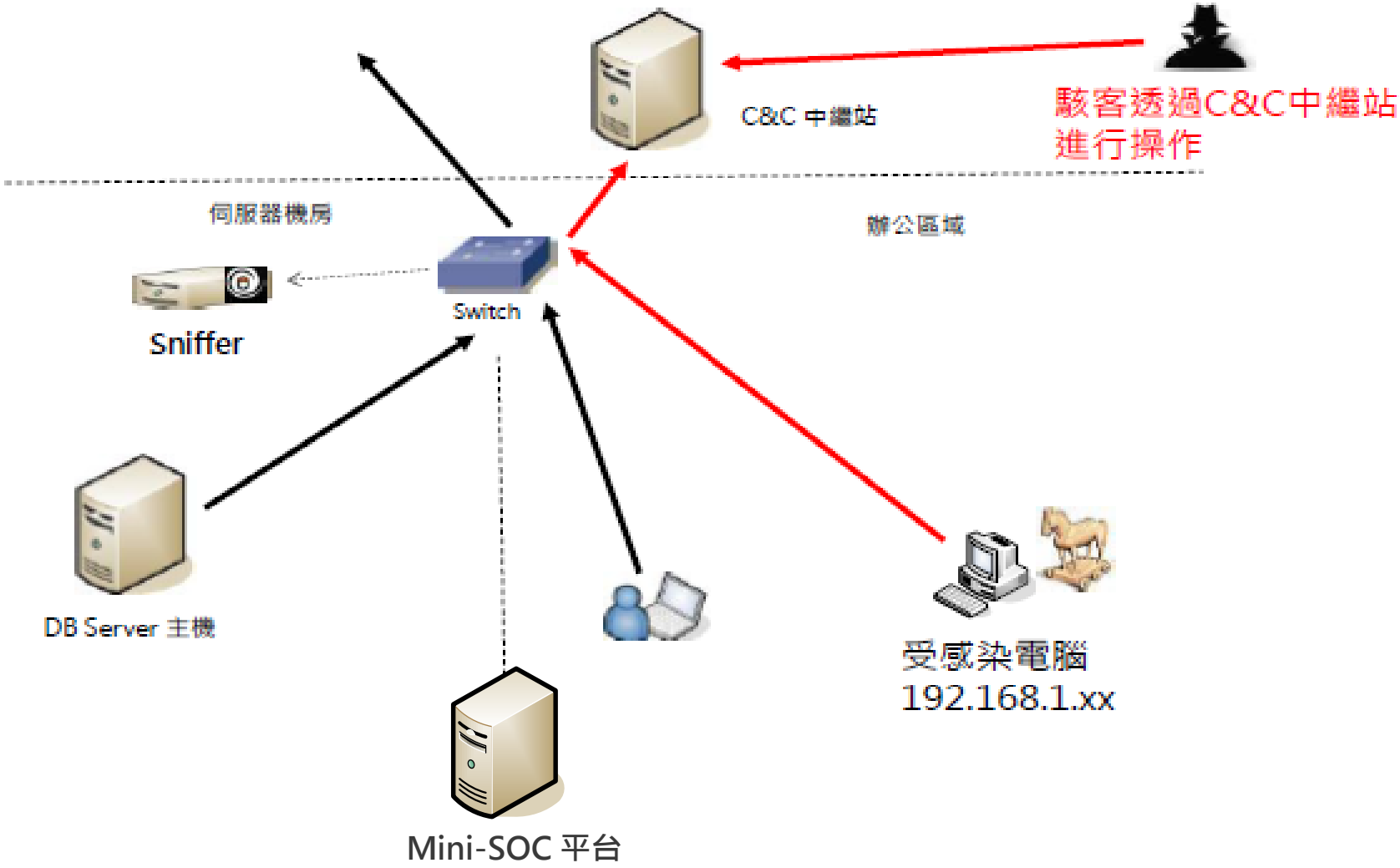
2.封包監聽與分析

採用之技術方法	檢視是否有以下網路惡意活動
1. 以Sniffer/IDS執行監聽側錄與分析封包	✓ 異常連線或DNS 查詢。 ✓ 是否連線已知惡意IP、中繼站(C&C) ✓ 有符合惡意網路行為的特徵。 ✓ 分析過濾異常連線紀錄。



- 透過專用網路設備側錄封包，收集前會與受測機關進行比對，確認流量是否與收錄的封包是否一致。現場可以直接進行分析，如有重大風險會先通報受測機關，封包收集回公司後會再做進一步的分析。
- 分析結果會與受測機關進行確認以降低誤判，封包分析主要以檢視受測機關的網路環境，是否有異常連線或惡意網路行為之特徵，並提出可能影響業務營運之潛在威脅。

(二)惡意中繼站清單


C&C 中繼站
駭客透過C&C中繼站
進行操作
伺服器機房
辦公區域
Switch
Sniffer
DB Server 主機
受感染電腦
192.168.1.xx
Mini-SOC 平台

(三) 資安健診（使用者端電腦檢視）

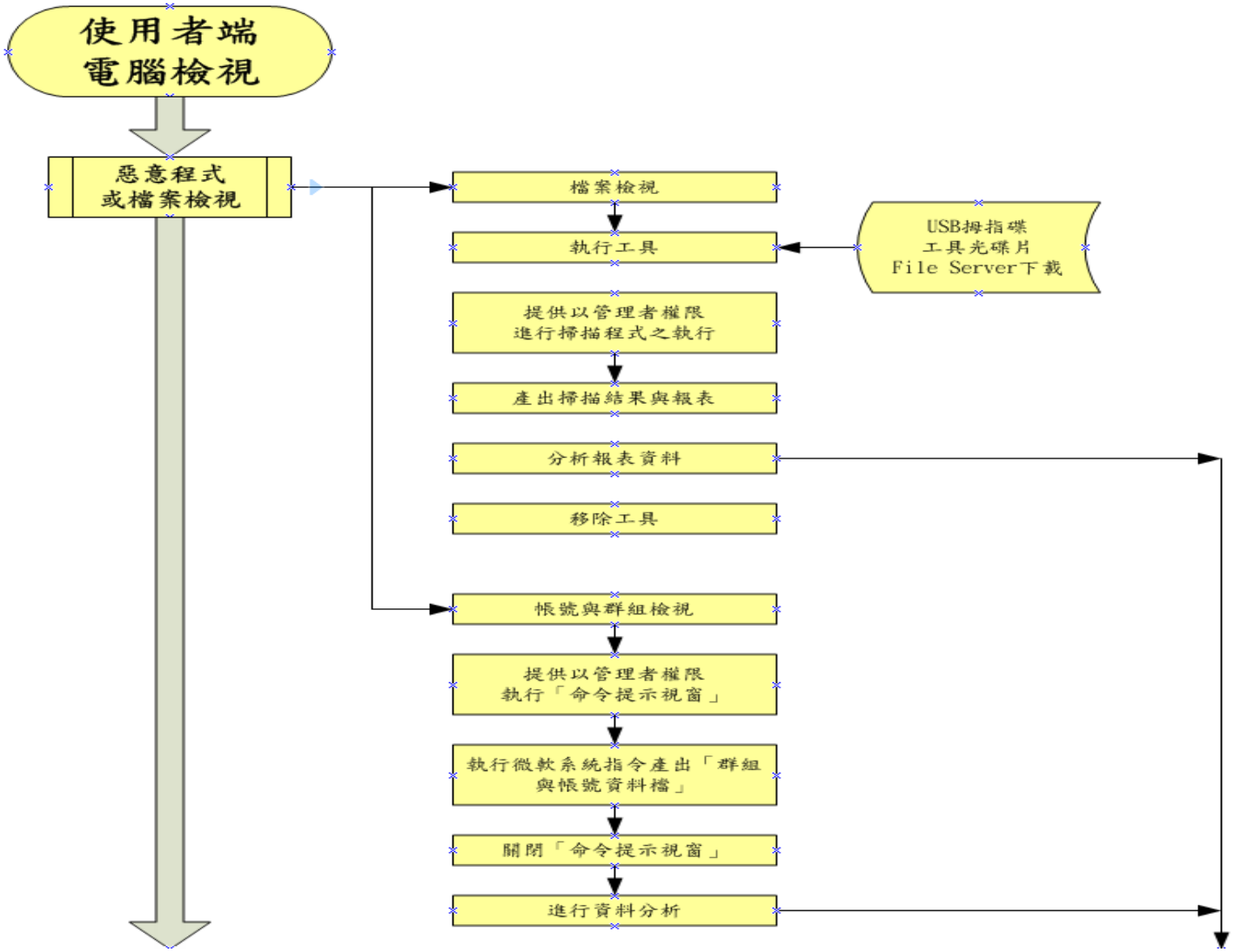
- **使用者端電腦惡意程式或檔案檢視針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目：**

1.活動中與潛藏惡意程式
2.駭客工具程式
3. 異常帳號與群組
4. 政府組態基準

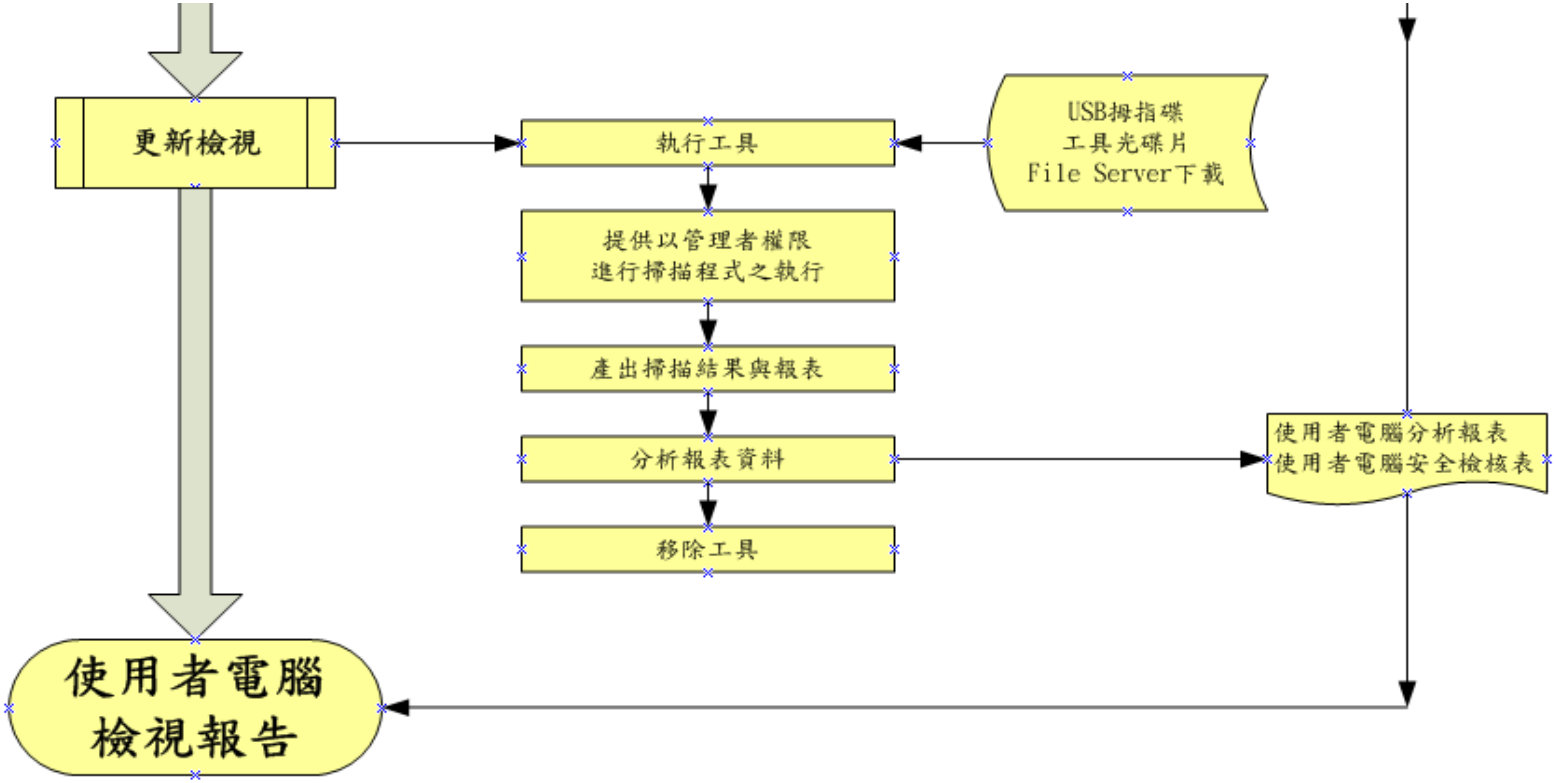
- **使用者電腦更新檢視應用程式更新檢視**

1.作業系統
2.Office 應用程式
3.防毒軟體
4.Adobe Acrobat
5.Adobe flash player

(三) 資安健診 (使用者端電腦檢視)



執行方式 - 資安健診（使用者端電腦檢視）



(三)端末電腦安全檢測/安全設定檢視

1	症狀檢查	是否有遭駭客建立OS帳號
2		是否無法開啟隱藏資料夾
3		Windows防火牆是否允許未知的服務
4		是否有可疑異常的隱藏系統檔
5		是否有異常連線
6		透過異常路徑檢查可疑exe,dll: 檢查exe及dll執行路徑是否在temp資料夾中執行
7		是否開機啟動載入異常程式
8		是否有異常Process
9	DLL injection 檢查	DLL injection 檢查
10	自動化工具掃描	自動化工具
11	可疑檔案分析與採樣	checkscan1-2.8報告是否產生可疑,檔案是否收集
12		可疑異常的隱藏系統檔是否收集
13		可疑的Process 或 dll 檔案是否收集
14		未通過系統簽章的檔案是否收集

(三)使用者端電腦電腦惡意程式檢視

針對個人電腦與伺服器主機端進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

- 事件記錄檔檢查(eventlog)

電腦稽核記錄內包含使用者登入登出、Windows 記錄、應用程式及服務記錄檔，可由事件記錄檔檢視電腦是否有異常行為。

(三)使用者端電腦電腦惡意程式檢視

- 系統記錄檔檢查(syslog)

電腦目前正在執行的記錄，可透過此記錄了解目前系統正在執行的程式中是否含有可疑程式。

- 本機使用者和群組檢查

系統登入使用者帳號及群組，駭客常利用提升權限或是新增使用者方式，增加系統使用者帳號並利用此帳號進行操作電腦，檢視是否電腦中有異常的群組或是使用者。

(三)使用者端電腦電腦惡意程式檢視

- 系統啟動區檢查

檢視系統設定啟動中，是否有異常的程式或是設定，惡意程式多會寫入啟動區中，透過系統開啟時及自行啟動惡意程式。

- 電腦機碼檢查

電腦在執行任意程式均分成電腦機碼及應用程式兩部份，檢視電腦機碼是否有異常內容，並操作系統中隱藏的程式。

(三)使用者端電腦電腦惡意程式檢視

- 設定檔檢查(XML)

檢視電腦中記錄檔設備是否有被更改，主要檢視網站XML檔案及系統hosts檔案。hosts檔案主要為電腦連線domain與IP對應， 惡意常針對此檔案更改內容以躲避單位防護設備偵測。

- 啟動項目檢查

檢查啟動項包含啟動資料夾、Run、RunOnce 和其他登錄機碼中的程式。

(三)使用者端電腦電腦惡意程式檢視

- 工作管理員檢查

列出目前電腦中正在運行的全部程式以及跟運行中程式相關的全部詳細資料，找出哪些程式佔用最多CPU資源、哪些執行序用掉最多記憶體以及那些程式目前有連線行為。

- Tcpview檢查

列出本機電腦的全部對外連線狀況，跟「netstat」指令很像。如果你想知道某個軟體是否有透過什麼樣的方式對外連線、送出或接收資訊的話，只要木馬在記憶體中運行，一定會開啟某個連接埠，只要駭客進入你的電腦，就有新的執行緒可利用連線行為偵測木馬行為。

(三)使用者端電腦電腦惡意程式檢視

- 工作管理員檢查

列出目前電腦中正在運行的全部程式以及跟運行中程式相關的全部詳細資料，找出哪些程式佔用最多CPU資源、哪些執行序用掉最多記憶體以及那些程式目前有連線行為。

- Tcpview檢查

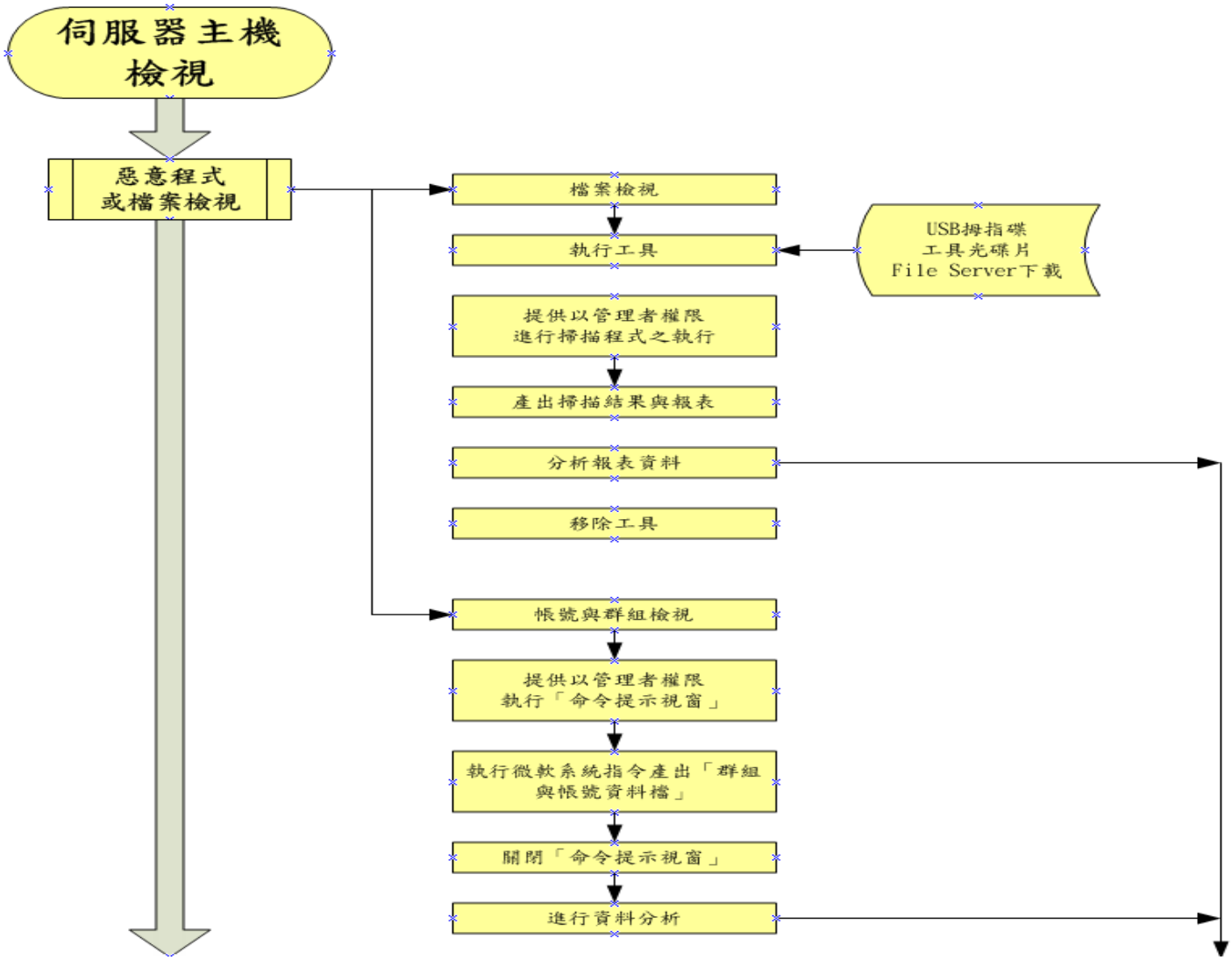
列出本機電腦的全部對外連線狀況，跟「netstat」指令很像。如果你想知道某個軟體是否有透過什麼樣的方式對外連線、送出或接收資訊的話，只要木馬在記憶體中運行，一定會開啟某個連接埠，只要駭客進入你的電腦，就有新的執行緒可利用連線行為偵測木馬行為。

(四)伺服器主機檢視

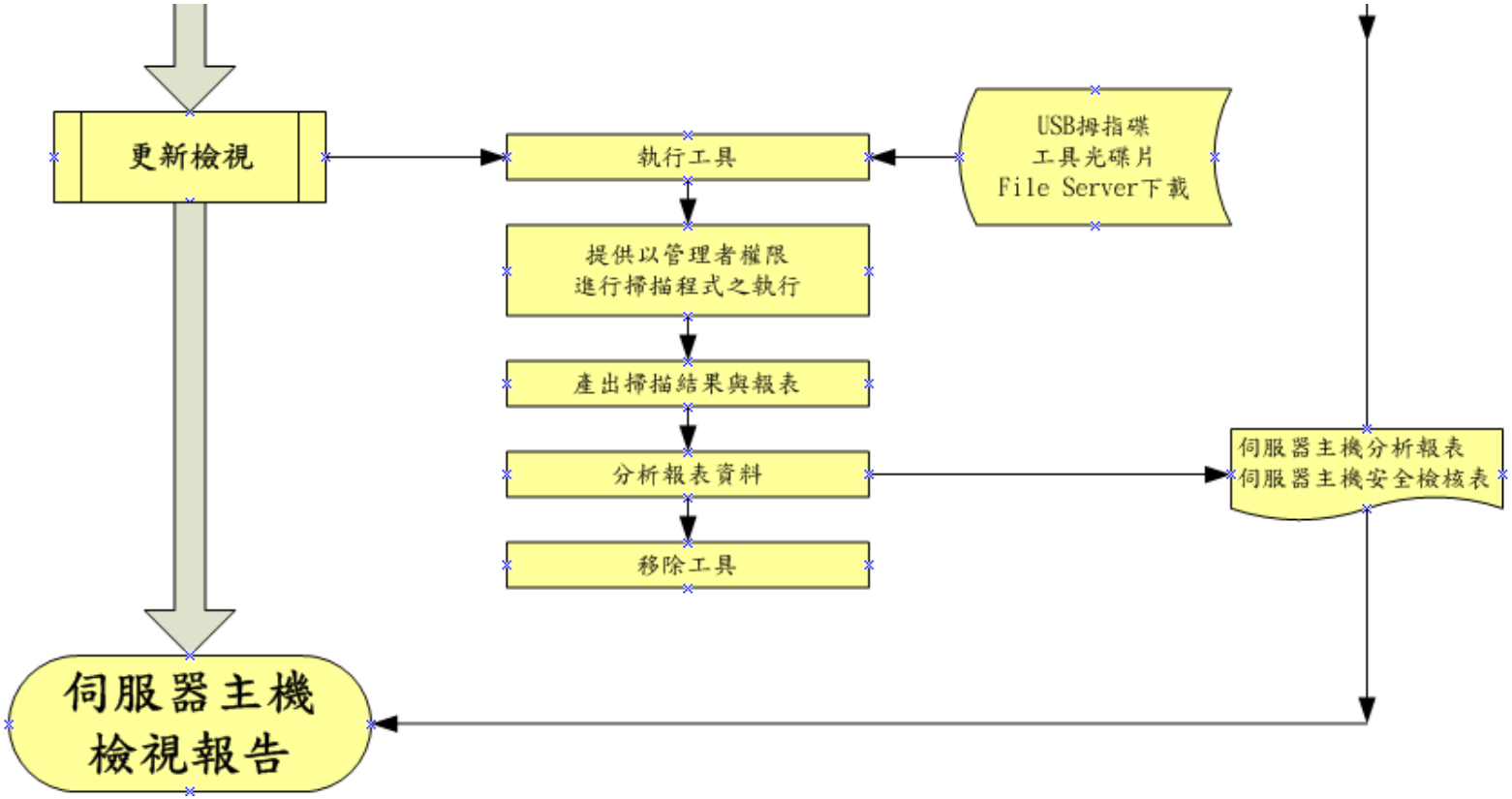
- **伺服器電腦惡意程式或檔案檢視針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目：**
  1. 活動中與潛藏惡意程式
  2. 駭客工具程式
  3. 異常帳號與群組

- **伺服器電腦更新檢視應用程式更新檢視**
  1.作業系統
  2.Office 應用程式
  3.防毒軟體
  4.Adobe Acrobat
  5.Adobe flash player

執行方式 - 資安健診（伺服器主機檢視）



執行方式 - 資安健診（伺服器主機檢視）



項次	檢視項目	備註
(1)	網站記錄檔(web_log)	
(2)	事件記錄檔檢查(event_log)	
(3)	系統記錄檔檢查(syslog)	
(4)	本機使用者和群組(user/group)	
(5)	系統啟動區(msconfig)	
(6)	電腦機碼檢查(regedit)	
(7)	系統上傳目錄(upload_file)	
(8)	開啟文件記錄(file_log)	
(9)	設定檔(config)	
(10)	啟動項目(run_list)	
(11)	工作管理員(Process)	
(12)	Tcpview(netstat)	
(13)	是否無法開啟隱藏資料夾	
(14)	Windows 防火牆是否允許未知的服務	//檢查 Windwos 防火牆的狀態 //檢查 Windwos 防火牆允許的程式清單
(15)	是否有可疑異常的隱藏系統檔	
(16)	是否有異常連線	
(17)	DLL injection 檢查	
(18)	(網站伺服器) WebShell 掃瞄	
(19)	(網站伺服器) 網頁備份檔遺留檢查	

(五)安全設定檢視

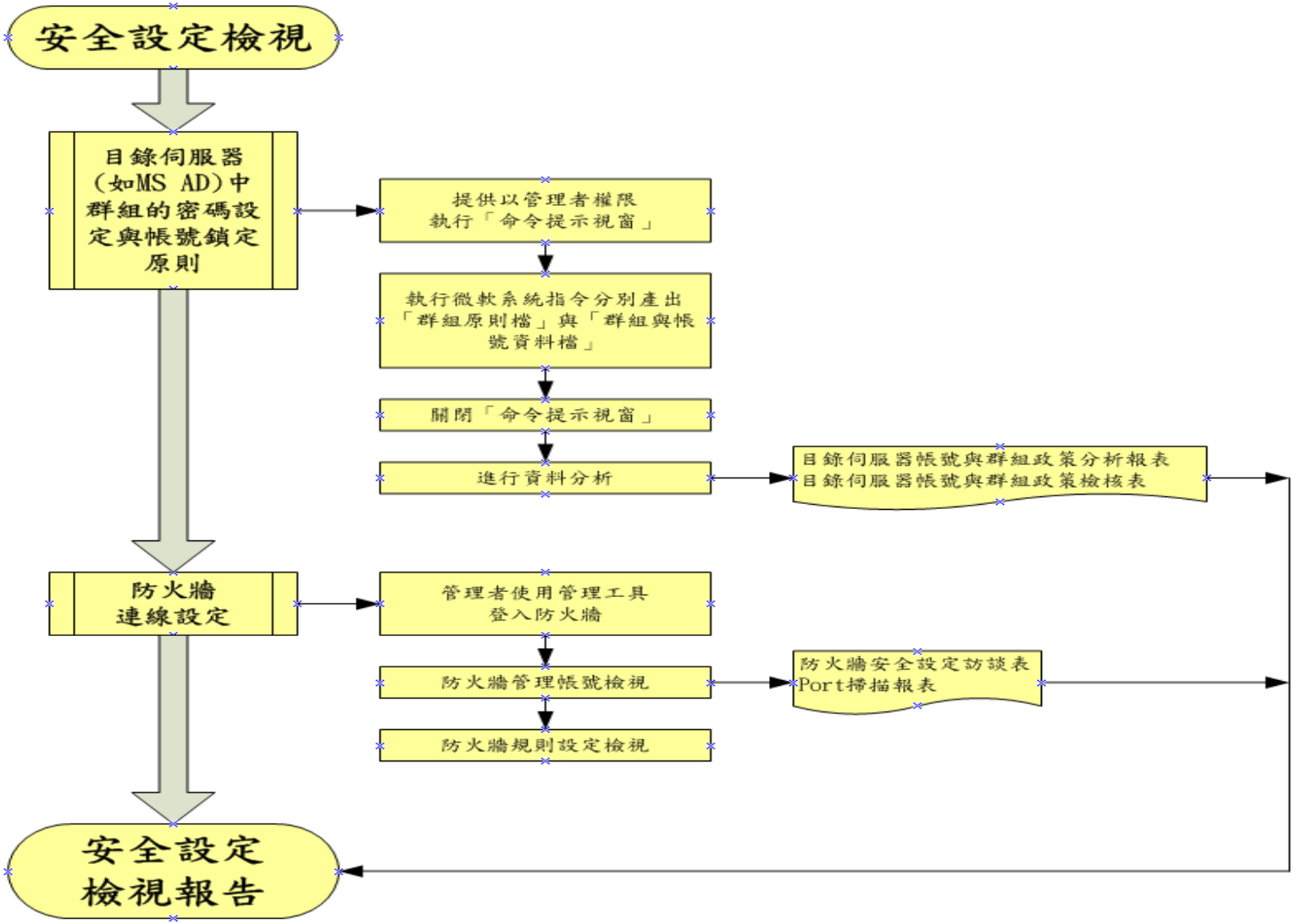
- 目錄伺服器(如MS AD)中群組的密碼設定與帳號鎖定原則 檢視目錄伺服器中群組的密碼設定與帳號鎖定原則，例如

1. AD伺服器有關群組原則(Group Policy)中之「密碼設定原則」與「帳號鎖定原則」設定
2. 若無AD伺服器，可以其他目錄伺服器(如LDAP)或以個別使用者端電腦檢視方式完成「密碼設定原則」與「帳號鎖定原則」安全設定檢視(使用者端電腦以項次3的電腦為範圍)

- 防火牆連線設定檢視防火牆

1. 是否開啟具有安全性風險的通訊埠或非必要通訊埠
2. 連線設定是否有安全性弱點

(五)執行方式 - 資安健診 (安全設定檢視)



應辦事項-技術面

辦理項目	辦理內容	A	B	C
資通安全防護(啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	1年內	1年內
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆(WAF)	1年內	1年內	
	APT攻擊防禦	1年內		
政府組態基準	依主管機關公告之項目，完成政府組態基準導入作業，並持續維運(公務機關)	1年內	1年內	

政府組態基準(GCB)政策說明

GCB發展規劃(1/3)

- 「國家資通訊安全發展方案(102年至105年)」行 動方案2.3.2.「推展資安基礎環境安全設定」執 行要點如下：
  a. 持續規劃不同系統政府組態基準設定
  b. 針對服務目錄網域環境與單機作業環境，分別設計其組 態部署機制
  c. 針對政府組態基準辦理教育訓練
- GCB發展規劃
  a. 依據各部會及所屬機關之使用者電腦常用作業系統與應用程式為優先發展方向
  b. 未來伺機擴及伺服器主機與網通設備

GCB發展規劃(2/3)

年度	發展情形
102	• 發展Windows 7與IE 8之政府組態基準(GCB) • 針對Windows 7與IE 8，設計服務目錄網域環境(Active Directory)與單機作業環境(Local)之組態部署機制 • 辦理Windows 7與IE 8政府組態基準(GCB)之實作研習活動教育訓練
103	• 發展Windows Server 2008 R2與Red Hat Enterprise Linux 5(RHEL 5)之政府組態基準(GCB) • 針對Windows Server 2008 R2設計服務目錄網域環境(Active Directory)與單機作業環境(Local)之組態部署機制 • 針對RHEL 5設計單機與網路之組態部署機制 • 持續辦理Windows 7與IE 8政府組態基準(GCB)之實作研習活動教育訓練
104	• 發展Windows 8.1、IE 11與無線網路之政府組態基準(GCB) • 針對Windows 8.1與IE 11設計服務目錄網域環境(Active Directory)與單機作業環境(Local)之組態部署機制 • 辦理Windows Server 2008 R2、IE 11及RHEL5政府組態基準(GCB)之實作研習活動教育訓練

GCB發展規劃(3/3)

- 已發展完成之政府組態基準(GCB)
  a. Windows 7、Windows Server 2008 R2(WS2008R2)
  b. IE 8、IE 11
  c. Red Hat Enterprise Linux 5 (RHEL5)
- 發展中之政府組態基準(GCB)
  a. Windows 8.1
  b. 無線網路

GCB相關政策說明(1/3)

- 各機關儘早導入政府組態基準(GCB)設定。請各部會務必於本(102)年底前，完成Windows7或IE8環境導入政府組態基準(GCB)設定及現行系統取得ActiveX簽章等作業；對於新建置之客製化軟體，則應將ActiveX安全性檢測（至少含弱點掃描、源碼檢測及滲透測試等必要項目）納為專案需求

GCB相關政策說明(2/3)

- 執行規劃
  a. 於行政院國家資通安全會報第25次委員會議中，由行政院資安辦提報整體辦理進度
- 長期規劃
  a. 擴及非Windows環境(Linux、Firefox、Chrome)
  b. 擴及其他設備(行動設備、網通設備)
  c. 推動元件安全性檢測作業(Active X、Plugins)

GCB相關政策說明(3/3)

- 環境規劃
  - a. 基本設定
    - ① Windows 7（不得降級使用）
    - ② IE 8
  - b. 實務考量
    - ① 各部會及所屬機關得依實務需求修訂基本設定，並進行例外管理，且將列為行政院國家資通安全會報資安稽核項目
    - ② 自103年1月1日起，系統開發廠商必須提出Active X 元件程式碼簽章證明
  - c. 教育訓練
    - ① 由技服中心規劃，自102年7月起常態辦理

Active X安全性機制(1/3)

- 程式碼簽章
  a. 透過在程式碼中加入數位憑證，以防止程式遭竄改、損毀或遭惡意程式感染
  b. 主要目的係在於確認各該Active X 元件開發廠商，並確認於簽署後，未經任何竄改
- 可驗證之數位憑證來源
  a. 政府憑證(GCA)、工商憑證、商用憑證

Active X安全性機制(2/3)

- 安全性檢測
  a. 利用弱點掃描、源碼檢測、滲透測試、模糊測試或迴歸測試等軟體檢測方法，確認Active X 元件是否存在可遭駭客控制軟體、竊取資料或癱瘓應用程式之弱點
  b. 檢測範圍可包含Active X 元件本身、 IE 設定檢測、資訊系統弱點檢測及作業系統環境等項目

Active X安全性機制(2/3)

- 檢測方式

項次	檢測方式	說明
1	弱點掃描	利用自動化弱點掃描工具，檢測受測軟體是否存在已知的應用程式弱點
2	源碼檢測	在不需要執行程式的情況下（也就是說程式並不需要上線運作），透過已知弱點特性的比對，針對原始碼內容進行分析，找出可能的弱點
3	滲透測試	以入侵者的思維方式，搭配掃描工具或攻擊程式之輔助，分析軟體可能存在之問題，並針對問題進行滲透的動作
4	模糊測試	利用自動化的方式將各種不合法的、不可預期的或是隨機亂數的輸入值傳送至受測軟體，以期能夠觸發錯誤條件或造成軟體功能失效，再利用錯誤條件挖掘潛在安全漏洞
5	迴歸測試	迴歸測試是指重複執行以前的全部或部分相同的測試工作，以確認之前已經測試過的軟體功能是否在軟體變更之後，仍然能夠運作正常

組態設定安全為重要的防護措施

- 美國網路安全協會2014年公布Twenty Critical Security Controls for Effective Cyber Defense (V5.1)

項次	Security Controls	相關資安弱點
1	Inventory of Authorized and Unauthorized Devices	• 未即時進行安全性更新 • BYOD
2	Inventory of Authorized and Unauthorized Software	• 未即時進行軟體更新 • 執行惡意軟體 • 侵犯智財權
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	• 不當的預設組態設定 • 預設帳號與弱密碼 • 預設啟用非必要服務
4	Continuous Vulnerability Assessment and Remediation	• 未定期執行弱點掃描 • 未即時進行弱點修補
5	Malware Defenses	• 未安裝防毒軟體 • 未即時更新病毒碼 • 使用來路不明軟體

防護案例

- 情境：使用者不小心將含有惡意程式的隨身碟插入公務電腦中
- 防護：
  a. 由於組態設定禁止可攜式媒體的自動播放功能，因此可降低電腦遭受惡意程式感染的機率
  b. 組態設定強制Windows之安全性更新保持在最新的狀態，因此可大幅減少惡意程式所能利用的漏洞
  c. 萬一不幸網域內其他電腦遭受惡意程式感染，組態設定禁止電腦回應廣播的封包，可避免惡意程式的感染範圍擴大

目的

政府組態基準(Government Configuration Baseline，簡稱GCB)目的在於規範資通訊終端設備(如：個人電腦) 的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

目的

- 正確的組態設定，可以降低系統管理權限遭提升之風險
- 正確的組態派送，可以快速的提升安全組態之符合程度，但可彈性的保留必要之組態，進行例外管理。

政府組態基準項目內容

- Windows 7+Internet Explorer 8
- Windows 8.1 + Internet Explorer 11
- Windows Server 2008 R2 SP1(網域控制站)
- Red Hat Enterprise Linux 5
- 無線網路說明

Windows7政府組態基準項目內容

- **Account Policy**
  a. 對於密碼原則、帳戶鎖定原則等組態進行檢測。
- **Computer Energy Policy**
  a. 電源管理原則組態進行檢測。
- **Computer Settings**
  a. 安全性選項
  b. 使用者權限指派
  c. 網際網路通訊設定
  d. 自動播放原則
  e. .....等

Windows7政府組態基準項目內容

- **Firewall Settings**
  a. Windows 防火牆公用設定檔、私人設定檔、網域設定檔等原則組態進行檢測。
- **Internet Explorer**
  a. Internet Explorer 內部網路區域、信任的網站區域等區域進行 JAVA 權限、登入選項、ActiveX 控制項等設定檔等原則組態進行檢測。

Windows7政府組態基準項目內容

- **User Settings**
  a. 使用者的安全控制項等設定檔等原則組態進行檢測
- **Security Patches**
  a. 作業系統的安全性修補安裝的狀態組態進行檢測

Windows7政府組態基準項目內容

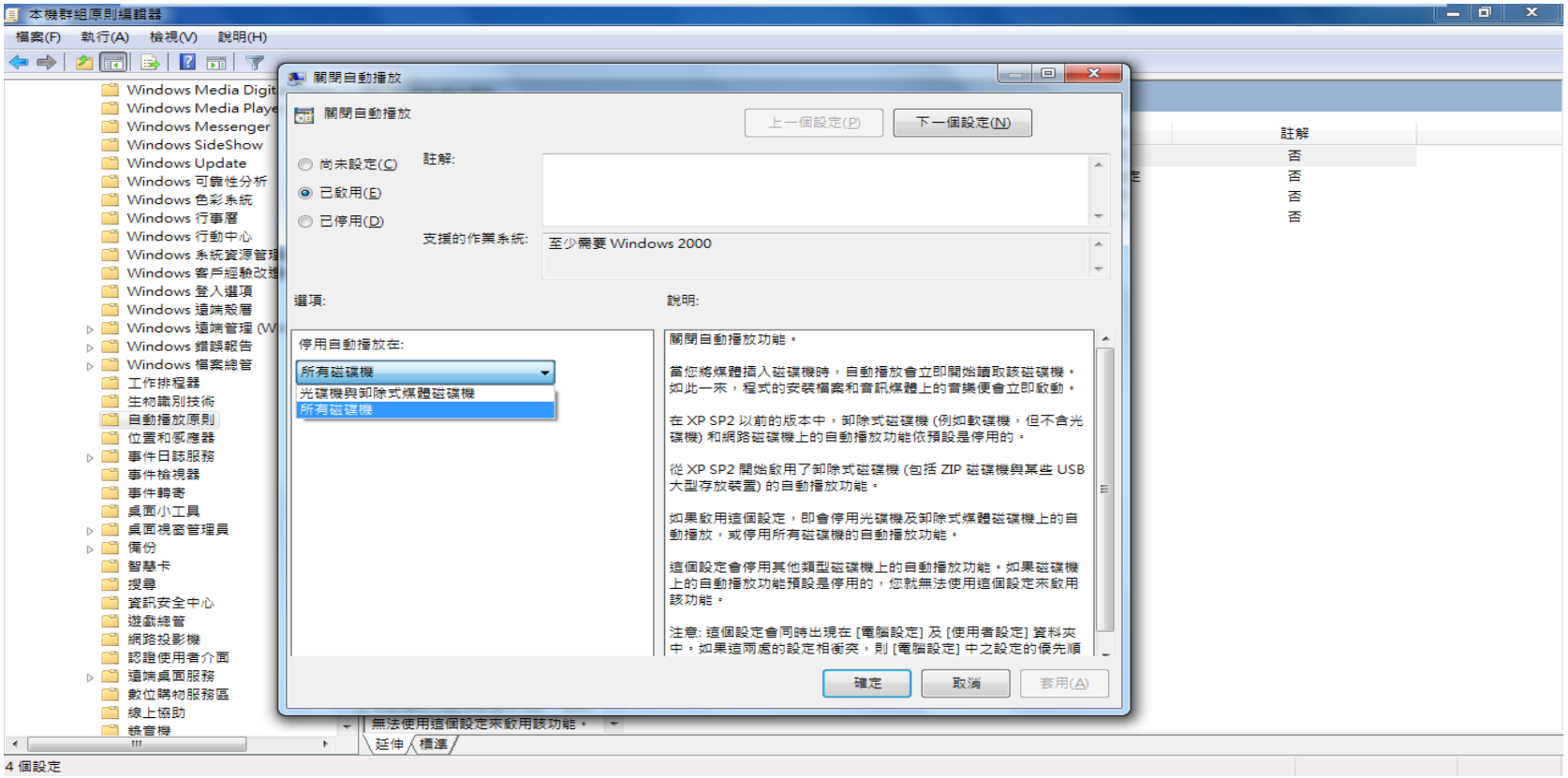
- **Windows 7、Windows 7 Firewall及Internet Explorer 8等3個基準設定**

項次	類別	項目名稱	項數	小計
1	Windows 7	USGCB Account Policy	9	246
		USGCB Windows 7 Computer Energy Policy	4	
		USGCB Windows 7 Computer Settings	225	
		USGCB Windows 7 User Settings	8	
2	Windows 7 Firewall	USGCB Windows 7 Firewall Settings	35	35
3	Internet Explorer 8	USGCB Internet Explorer 8 Computer Settings	110	115
		USGCB Internet Explorer 8 User Settings	5	
合計				396

Windows7政府組態基準分類

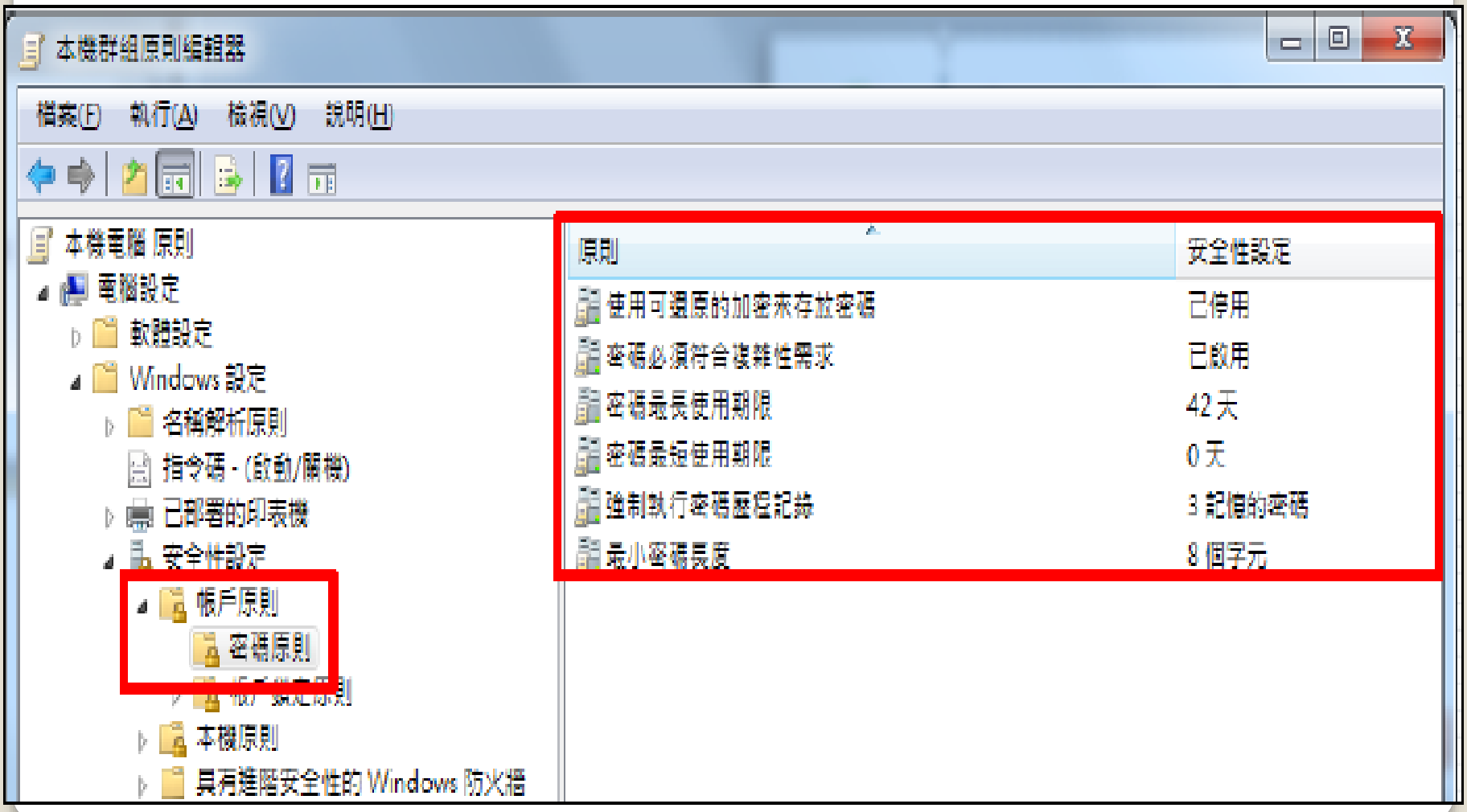
Windows7 GCB設定項目

- 群組原則編輯器 (gpedit.msc)
  1. 啟用原則 / 停用原則 / 尚未設定



Windows7 GCB設定項目

- 密碼原則



例外管理

- 所屬機關導入政府組態基準(GCB)時，得依實務需求修訂基本設定，並將列為行政院國家資通安全會報資安稽核項目

申請日期	104年7月1日	申請單位	資訊處	申請人	
例外管理項目					
項次	CCE-ID	規則名稱	基準值	變更值	變更理由	配套措施
範例	CCE-9357-5	密碼長度最小值	12字元	8字元	現有ISMS政策規範密碼長度為8碼，故暫時保留原設定值	待ISMS管理審查會議進行密碼長度變更為12碼之討論後，依決議結果調整ISMS政策規範及密碼長度設定
權責主管			核准日期		年 月 日	
執行人員			執行日期		年 月 日	
申請人確認			確認日期		年 月 日	

技服提供

例外管理注意事項

- 該項目於技服中心網站公告之「政府組態基準文件」中所表列之項目，應列入例外管理項目
  a. 如：有CCE-ID之項目(如：防火牆輸入/輸出規則)
- 該項目不於「政府組態基準文件」表列項目中，則無需納入例外管理項目
  a. 如：IE瀏覽器之信任網站(建議仍應具審核機制)

政府組態基準(GCB)相關資源

- 政府組態基準內容、GPO檔案、教育訓練教材及相關部署工具已公告於技服中心網站(www.icst.org.tw)之「政府組態基準(GCB)」專區，供機關下載使用

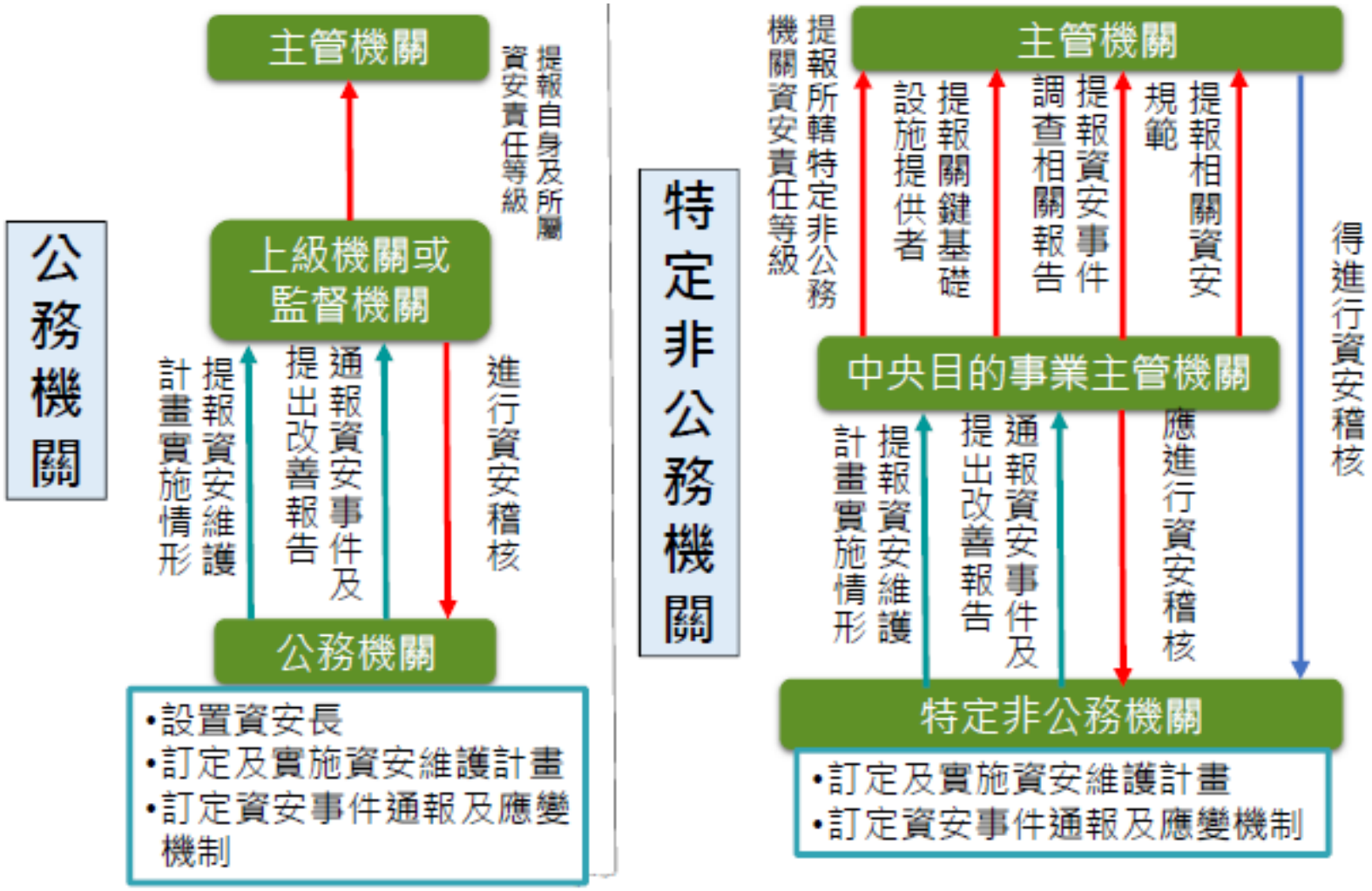
應辦事項-認知與訓練

辦理項目	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每年接受之資通安全專業課程訓練或資通安全職能訓練	4名各12小時	2名各12小時	1名12小時
	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	3小時	3小時	3小時
資通安全專業證照及職能訓練證書	初次受核定或等級變更後之一年內，資通安全專職(責)人員總計應持有之資通安全專業證照，並持續維持證照之有效性	4張	2張	1張
	資通安全專職人員總計應持有之資通安全職能評量證書，並持續維持證照之有效性(公務機關)	4張	2張	1張

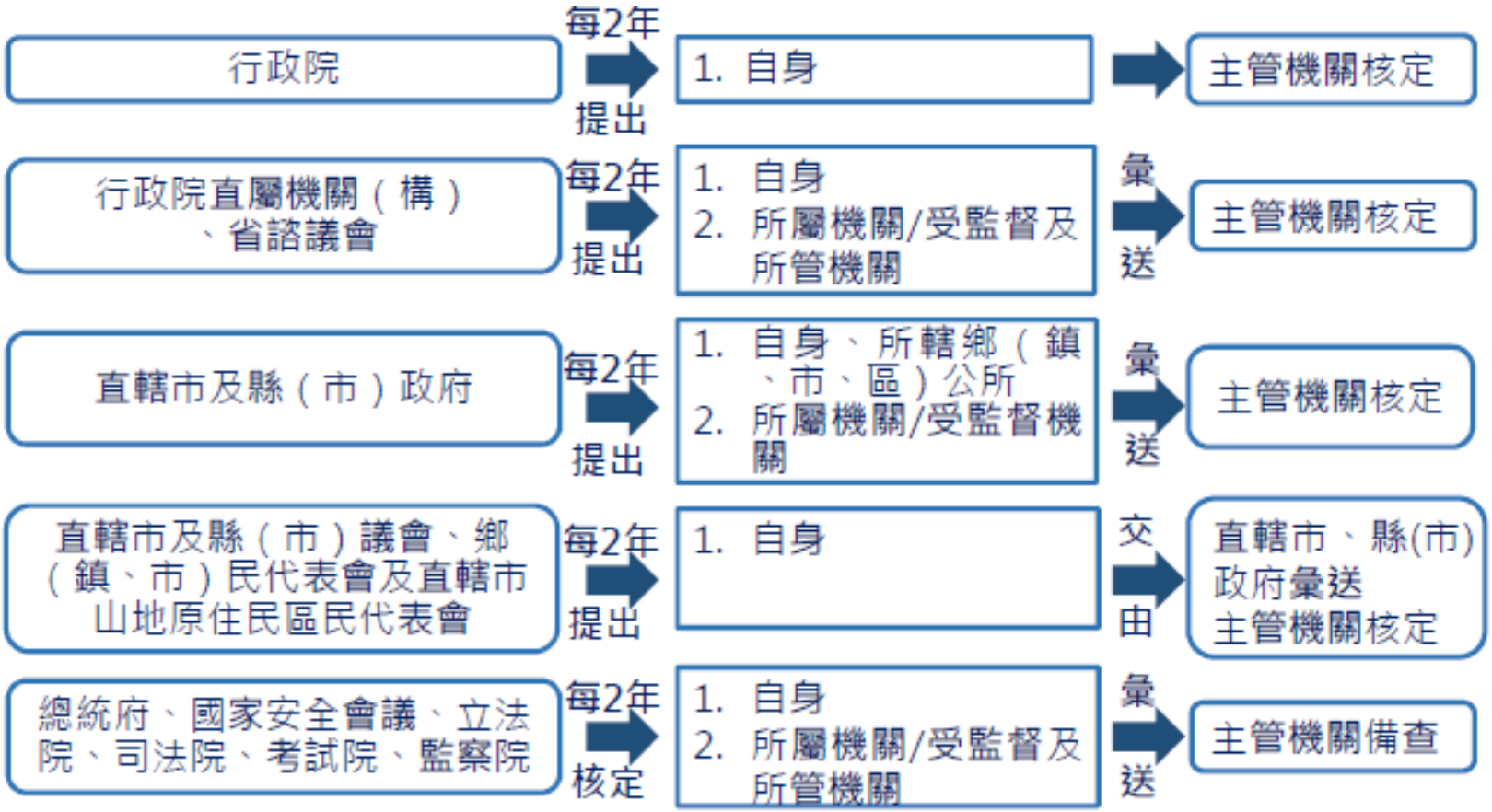
應辦事項-D級與E級

面向 作業 名稱 等級	技術面	認知與訓練
	資通安全防護	資通安全教育訓練
D級	初次受核定或等級變更後之一年內，完成下列資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級 一、防毒軟體 二、網路防火牆 三、具有郵件伺服器者，應備電子郵件過濾機制	一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練
E級		一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練

公務機關間之角色與權責

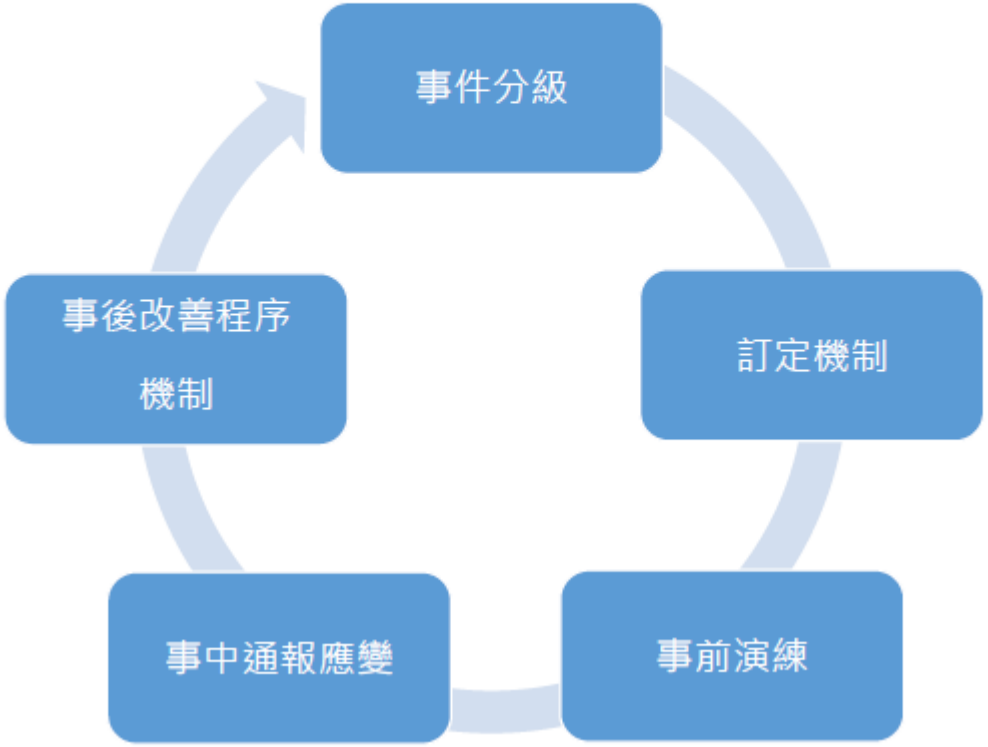


資通安全責任等級分級程序



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。



資通安全事件情資分享機制

情資分享

資通安全事件通報機制

其他情資

行政院建立資通安全情資分享機制

行政院、上級機關

中央目的事業主管機關

經濟部、交通部、金管會及通傳會等

公務機關資通安全事件通報(§13)(強制通報)

公務機關

非公務機關資通安全事件通報(§17)(強制通報)

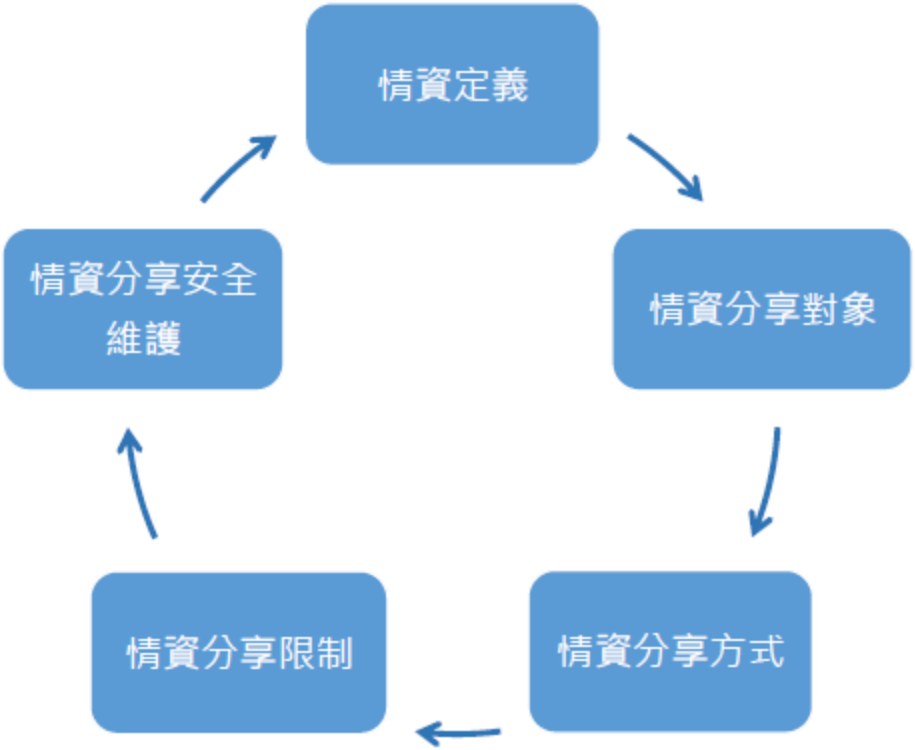
關鍵基礎設施提供者 ＋ 公營事業、政府捐助之財團法人

非公務機關資通安全事件通報(自願通報)

所有非公務機關

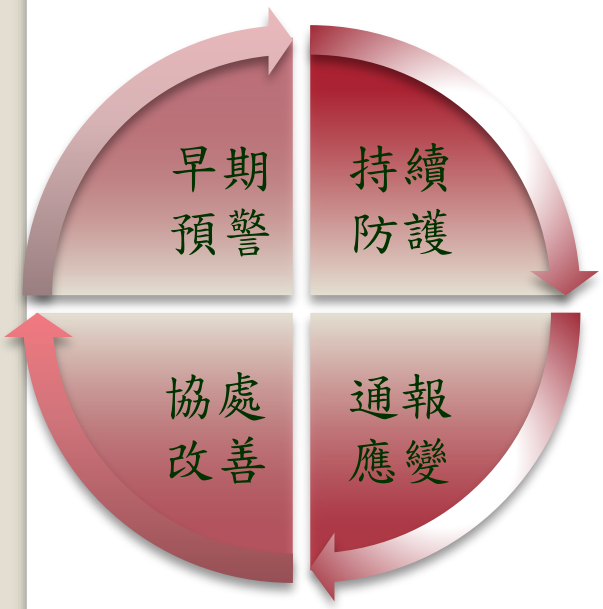
資通安全情資分享辦法

- 提升各機關對於資安之預警能力，強化資安相關資訊之交流。



資安聯防

使關鍵基礎設施**八大領域**均完成資安**四大面向**整備，建立情報驅動(Intelligence-based)之國家層級資安聯防架構



四大面向

X

八大領域

=

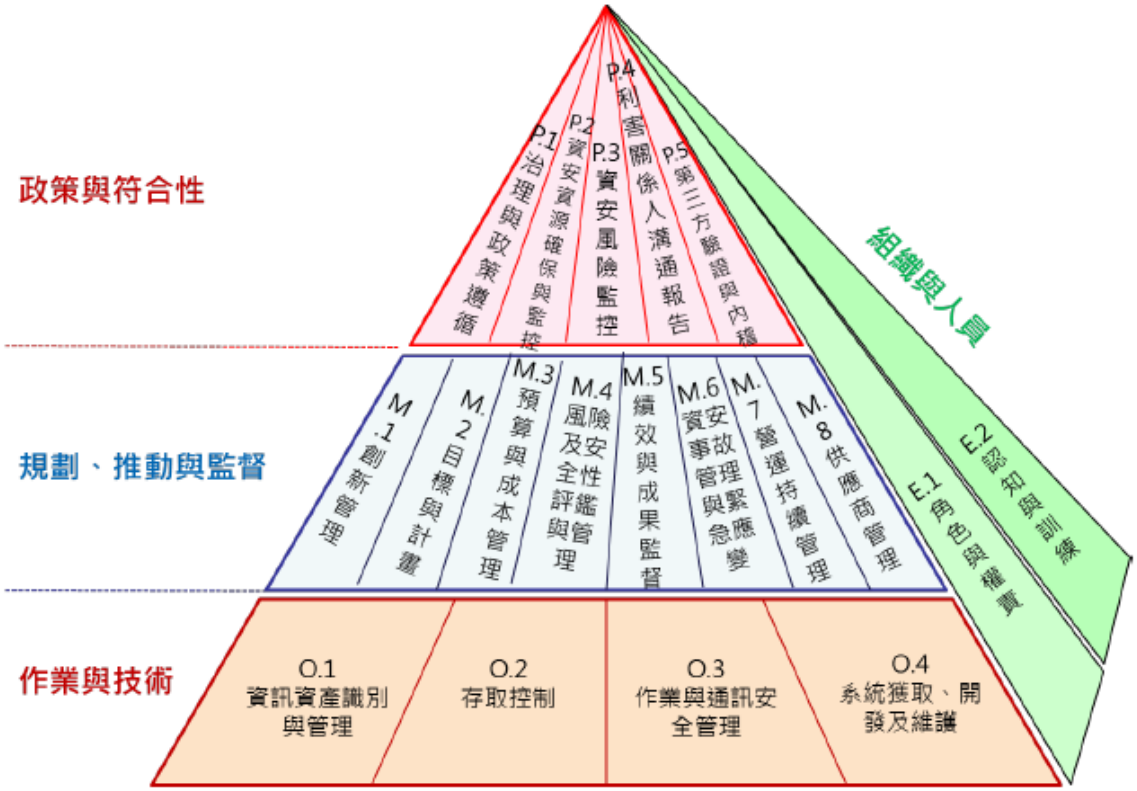
國家資安聯防架構

資安情報驅動三屬性

- 能見度(Visibility)
- 分析能量(Analysis)
- 快速行動(Action)

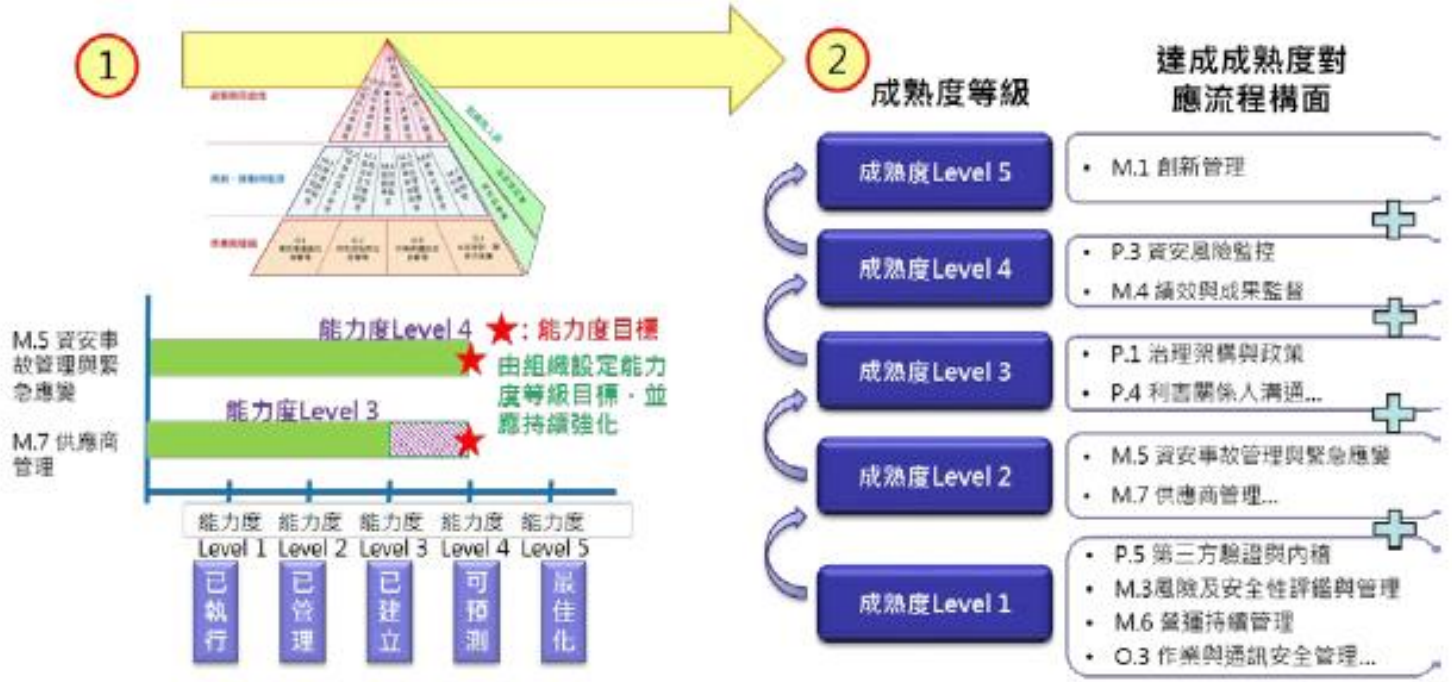
資安治理流程構面關係

依據資安治理架構模型之運作，各機關內的資安治理應與管理緊密配合並屬有關聯關係。以資安資源管理考量為例，在政策與符合性管理面向，資安治理強調組織整體之資安資源管理；在規劃、推動與監督面向

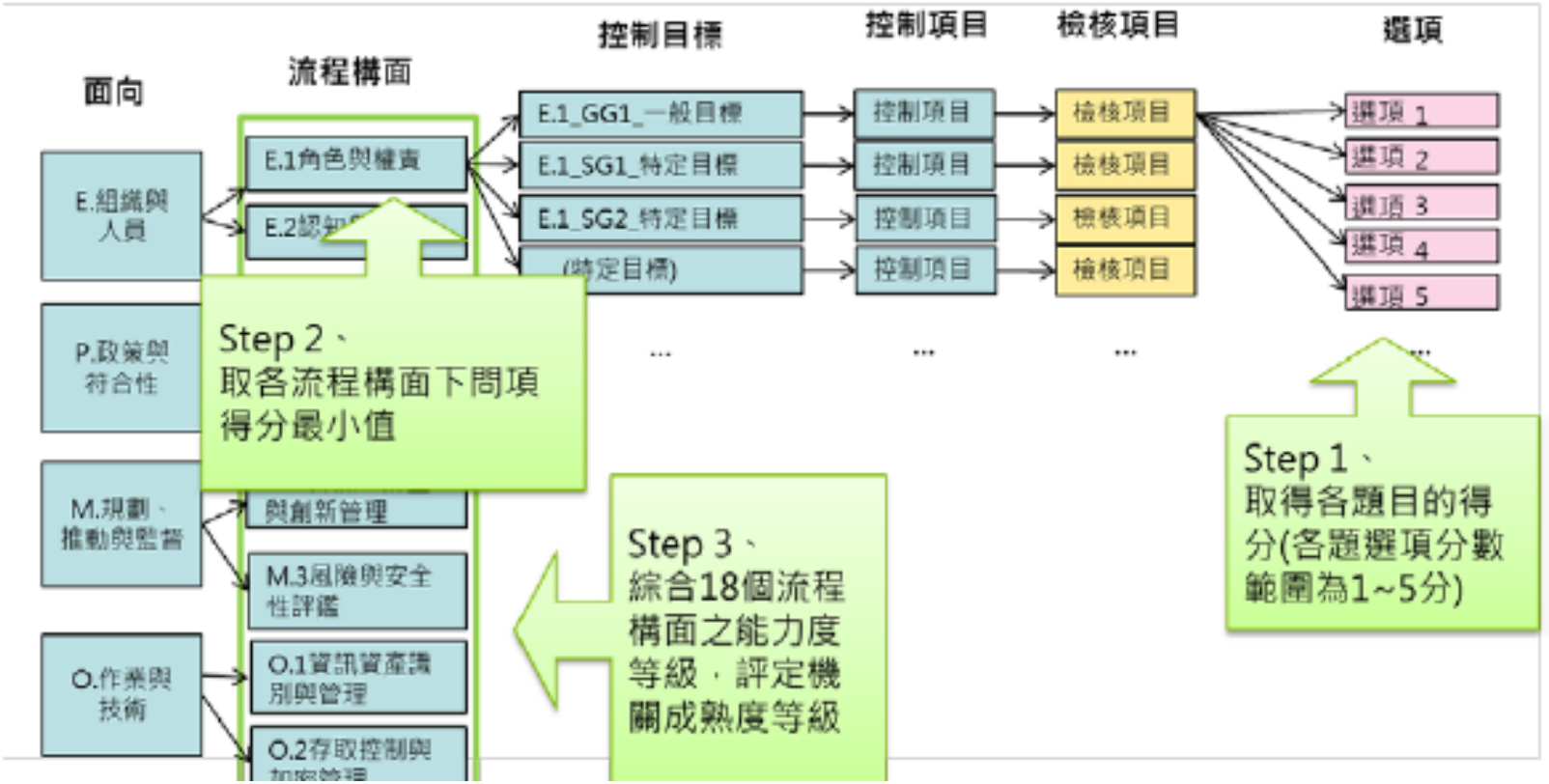


資安治理流程能力度與成熟度評審方法

- **能力度等級**：
  - 描繪組織流程於**特定**流程構面中的狀態
  - 以評審各流程構面之能力度
- **成熟度等級**：
  - 描繪組織的整體狀態
  - 用以評審組織之成熟度

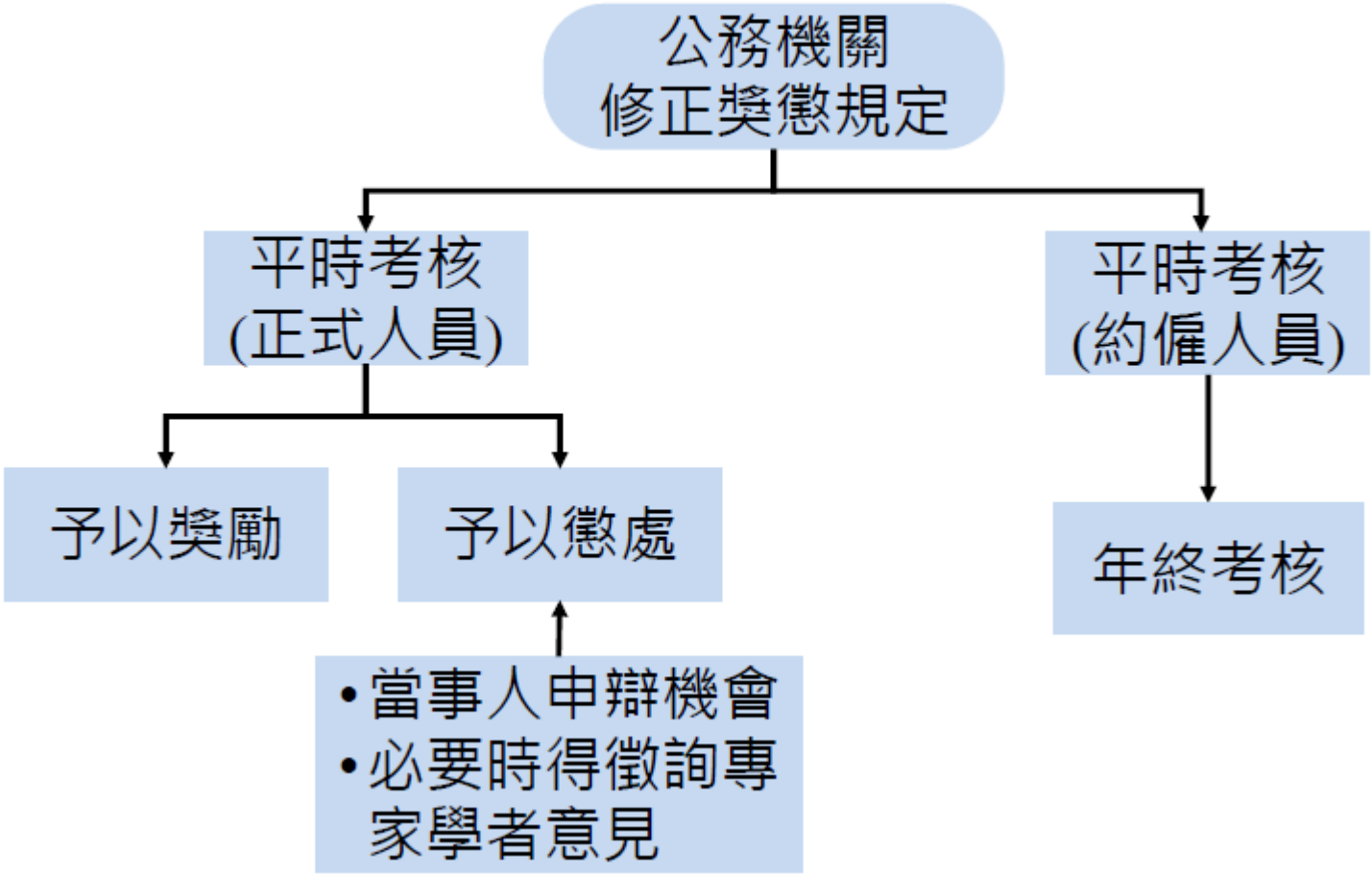


資安治理流程能力度與成熟度評審方法



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



作業建議事項


落實資安宣導
－機關內資安意識宣導
－資安相關獎懲規定
內部資安規範與本法之接軌
－機關內資安作業流程與規定之銜接
－人員獎懲規定之銜接
提升資安人員質與量
－重新檢視資安人力適足性
－指定資安專職、專責人力
－提升資安人員之職能
因應建議
1
2
3
4
5
檢視資安推動組織之組成
－組成跨機關內部單位及所屬機關
－形成與特定非公務機關之公私治理與參與模式
檢視資安預算之適足性

整備重點

註1：指上級、監督機關須針對所轄公務機關，就稽核作業訂定相關行政規則(依據母法第13條說明)
註2：指中央目的事業主管機關須針對所轄特定非公務機關，就資通安全維護計畫等應遵循事項訂定辦法(法規命令)(依據母法第16條第6項及第17條第4項)
註3：行政院會提供風險評鑑、資安維護計畫、通報應變機制等文件範本供參。

資通安全防護及控制措施

- 針對不需導入CNS27001之機關(範本)
  - 參考資安治理成熟度評審作業面向，CNS27002中控制措施之作業規範，提示原則性之準則(Standards)規範，請各依機關視實際情形增修，並針對各項準則定出相關程序(Procedures)文件

資訊及資通系統之管理	存取控制與加密機制管理	作業與通訊安全管理
	業務持續運作演練	
系統獲取、開發及維護	執行資通安全健診	資通安全防護設備

資通安全防護及控制措施

- 資訊及資通系統之管理
  - 資訊及資通系統之保管
    - 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級、持續更新
    - 資訊及資通系統管理人應確保資訊及資通系統被妥善保存或備份
    - 資訊及資通系統管理人應確保屬重要者，已採取適當之存取控制政策

資通安全防護及控制措施

- 資訊及資通系統之管理
  - 資訊及資通系統之使用
    - 使用資訊及資通系統前應經其管理人授權
    - 使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任
    - 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則
  - 資訊及資通系統之刪除或汰除
    - 刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統
    - 刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫
    - 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能

資通安全防護及控制措施

- 存取控制與加密機制管理

網路安全控管

- 定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級
- 網路區域應進行區隔(外部網路、非軍事區、內部網路)，各區域間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域
- 對於通過防火牆之來源端主機IP位址、目的端主機IP位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄
- DNS伺服器應設定指向GSN Cache DNS
- 機密資料原則不得透過無線網路及設備存取、處理或傳送

資通系統權限管理

- 資通系統應設置通行碼管理，通行碼之要求需滿足
  (1)通行碼長度8碼以上
  (2)通行碼複雜度應包含英文大小寫、特殊符號或數字兩種以上
  (3)使用者每90天應更換通行碼
- 使用資通系統前需經授權，並使用唯一之使用者ID，除有特殊營運或作業必要經核准並紀錄外，不得共用ID
- 無繼續使用資通系統時，應立即停用或移除使用者ID，資通系統管理者應定期清查使用者之權限

資通安全防護及控制措施

- 存取控制與加密機制管理

特權帳號之存取管理

- 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存
- 資通系統之特權帳號不得共用
- 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者ID
- 資通系統特權帳號應妥善管理，並應留存特殊權限帳號使用軌跡
- 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式

加密管理

- 加密保護措施應遵守下列規定
  (1)應落實使用者更新加密裝置並備份金鑰
  (2)應避免留存解密資訊
  (3)一旦加密資訊具遭破解跡象，應立即更改
- 機密資訊於儲存或傳輸時應進行加密

資通安全防護及控制措施

- 作業與通訊安全管理

防範惡意軟體控制措施

- 主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級
- 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查
- 使用者不得私自使用已知或有嫌疑惡意之網站
- 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊

遠距工作之安全措施

- 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形
  (1)提供適當通訊設備，並指定遠端存取之方式
  (2)進行遠距工作時之安全監視
  (3)提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊
- 資通安全推動小組應定期審查已授權之遠距工作需求是否適當
- 資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通

資通安全防護及控制措施

- 作業與通訊安全管理

電子郵件安全管理

- 人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用
- 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新
- 電子郵件管理及使用規定如下
  (1)系統管理人應定期清查電子郵件帳號
  (2)避免讀取來歷不明之郵件或含有巨集檔案之郵件，以防範社交工程攻擊
  (3)確保電子郵件傳送時之傳遞正確性
  (4)注意電子簽章之要求事項
  (5)純文字模式閱覽

確保實體與環境安全措施

- 資料中心及電腦機房之門禁管理
  (1)機關人員或來訪人員應申請及授權後，方可進入。管理者並應定期檢視授權人員之名單
  (2)人員及設備進出資料中心及電腦機房應留存紀錄
- 資料中心及電腦機房之環境控制
  (1)應安裝安全偵測及防護措施
  (2)各項安全設備應定期執行檢查、維修
- 辦公室區域實體與環境安全措施
  (1)考量採用辦公桌面淨空政策
  (2)機密性及敏感性資訊，不使用或下班時應該上鎖

資通安全防護及控制措施

- 作業與通訊安全管理

資料備份

- 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放
- 每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統
- 備份資料如有機密性考量，宜加密保護

媒體防護措施

- 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管
- 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄
- 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙

資通安全防護及控制措施

- 作業與通訊安全管理

電腦使用之安全管理

- 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體
- 電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等
- 下班時應關閉電腦及螢幕電源
- 電腦若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能

行動設備之安全管理

- 機密資料不得由未經許可之行動設備存取、處理或傳送
- 機敏會議或場所不得攜帶未經許可之行動設備進入

資通安全防護及控制措施

- 作業與通訊安全管理

即時通訊軟體安全管理

- 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理
- 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求
  (1)用戶端應有身分識別及認證機制
  (2)訊息於傳輸過程應有安全加密機制
  (3)應通過經濟部工業局訂定行動化應用軟體之中級檢測項目
  (4)伺服器端之主機設備及通訊紀錄應置於我國境內
  (5)伺服器通訊紀錄（log）應至少保存六個月

資通安全防護及控制措施

- **系統獲取、開發及維護**(有維護、自行或委外開發資通系統機關適用)
  - 資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求**分級**，依分級之結果，完成附表十中資通系統**防護基準**，並注意下列事項
    - 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle,SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」
    - 開發前設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形
    - 上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形
    - 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形

範例-某系統安全需求

- HTTPS傳輸加密
- 登入錯誤3次鎖定IP與帳號30分鐘
- 重設密碼功能使用圖形驗證碼(CAPTCHA)
- 網站下載資料提供HASH值供比對
- 系統程式與資料庫定時匯出備份至備援機
- 使用者輸入過濾特定SQL Injection惡意字元
- 密碼HASH過後儲存，不存純文字密碼
- 記錄使用者異動資料行為，保留原資料
- Log包含人事時地物
- 會談階段30分鐘失效
- 使用最新版函式庫，開啟port與服務最小化

軟體安全查檢表

OWASP - ASVS

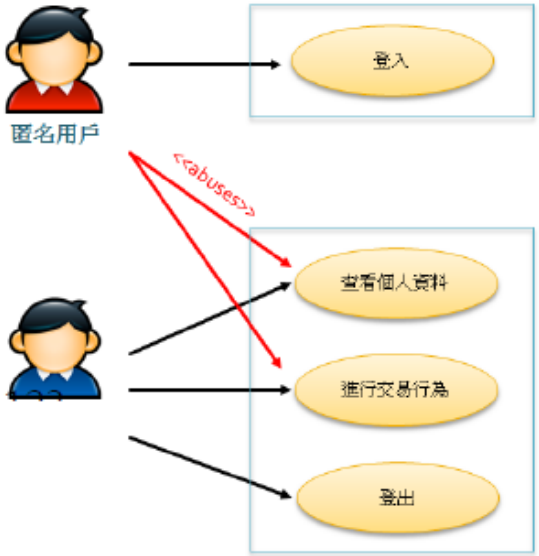
V2: Authentication Verification Requirements

The table below defines the corresponding verification requirements that apply for each of the verification levels. Verification requirements for Level 0 are not defined by this standard.

	AUTHENTICATION VERIFICATION REQUIREMENT	LEVELS 1	2	3
V2.1	Verify all pages and resources require authentication except those specifically intended to be public (Principle of complete mediation).	✓	✓	✓
V2.2	Verify all password fields do not echo the user's password when it is entered.	✓	✓	✓
V2.4	Verify all authentication controls are enforced on the server side.	✓	✓	✓
V2.5	Verify all authentication controls (including libraries that call external authentication services) have a centralized implementation.			✓
V2.6	Verify all authentication controls fail securely to ensure attackers cannot log in.	✓	✓	✓
V2.7	Verify password entry fields allow or encourage the use of passphrases, and do not prevent long passphrases or highly complex passwords being entered, and provide a sufficient minimum strength to protect against the use of commonly chosen passwords.		✓	✓
V2.8	Verify all account identity authentication functions (such as registration, update profile, forgot username, forgot password, disabled / lost token, help desk or IVR) that might regain access to the account are at least as resistant to attack as the primary authentication mechanism.		✓	✓
V2.9	Verify users can safely change their credentials using a mechanism that is at least as resistant to attack as the primary authentication mechanism.		✓	✓
V2.12	Verify that all authentication decisions are logged. This should include requests with missing required information, needed for security investigations.		✓	✓
V2.13	Verify that account passwords are salted using a salt that is unique to that account (e.g., internal user ID, account creation) and use bcrypt, scrypt or PBKDF2 before storing the password.		✓	✓

SANS – SWAT

誤用案例模型(Misuse Case)

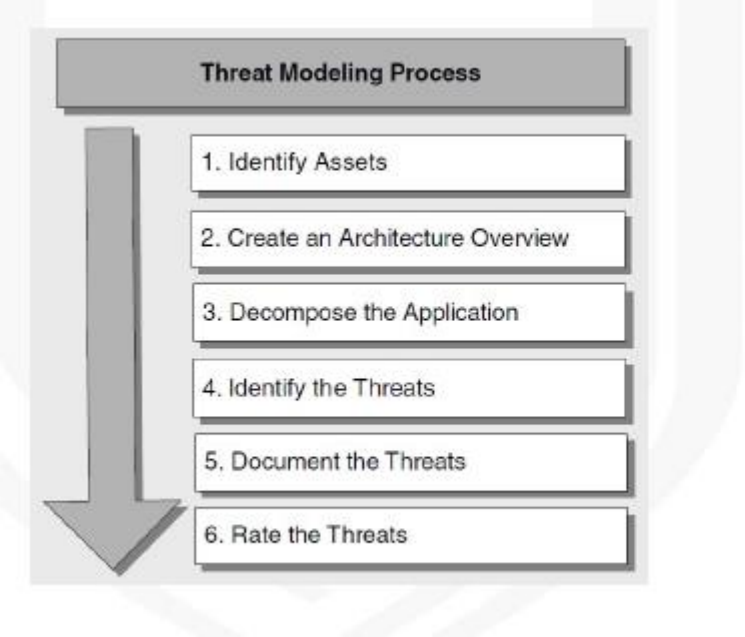


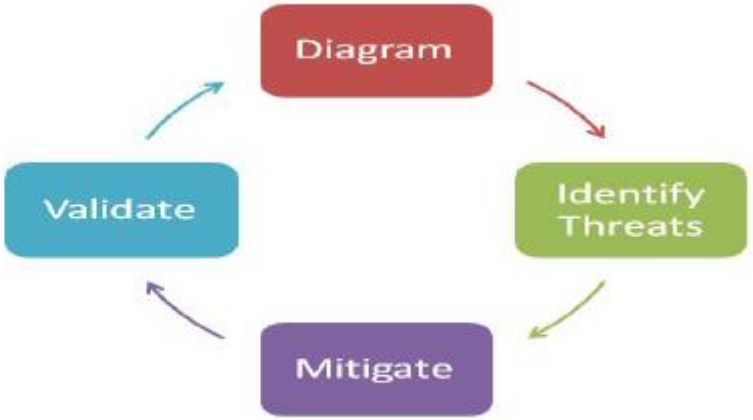
透過發展負面的使用情境來幫助識別安全需求
如何確保用戶只能存取查看個人資料?
- 每次存取要求都檢查其許可權
- 採用Server端的驗證授權機制，避免被繞過
- 避免直接顯示物件參考http://a.com/info?id=123

登入用戶的Session ID是否可能被劫奪進行偽冒交易
如何確保用戶只能存取查看個人資料?
- 會話識別字(Session ID)是隨機產生且不可預測
- 使用者的會話階段，設定在合理的時間內失效
- 使用者的會話識別字使用加密協定傳輸
- 使用者重新登入後，會話識別字(Session ID)會改變
- 不將會話識別字(Session ID)或使用者ID顯示於使用者可以改寫處

威脅建模(Threat Modeling)

- 威脅建模採用系統化的方法，以攻擊者角度，識別可能影響軟體系統的威脅並進行評估。
- 基於對架構與設計的瞭解，識別與評估威脅後，以風險高低的順序對威脅發展適當的控制措施





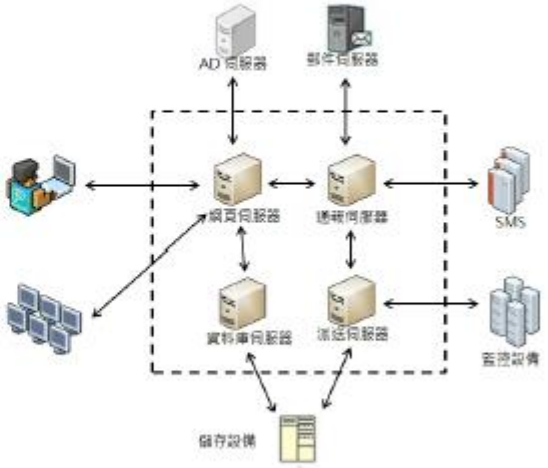
架構風險分析(Architecture Risk Analysis)

- 抗攻擊能力分析(Attack Resistance Analysis)
- 模糊分析(Ambiguity Analysis)
- 底層框架弱點分析(Underlying Framework Weakness Analysis)

抗攻擊能力分析 (Attack Resistance Analysis)

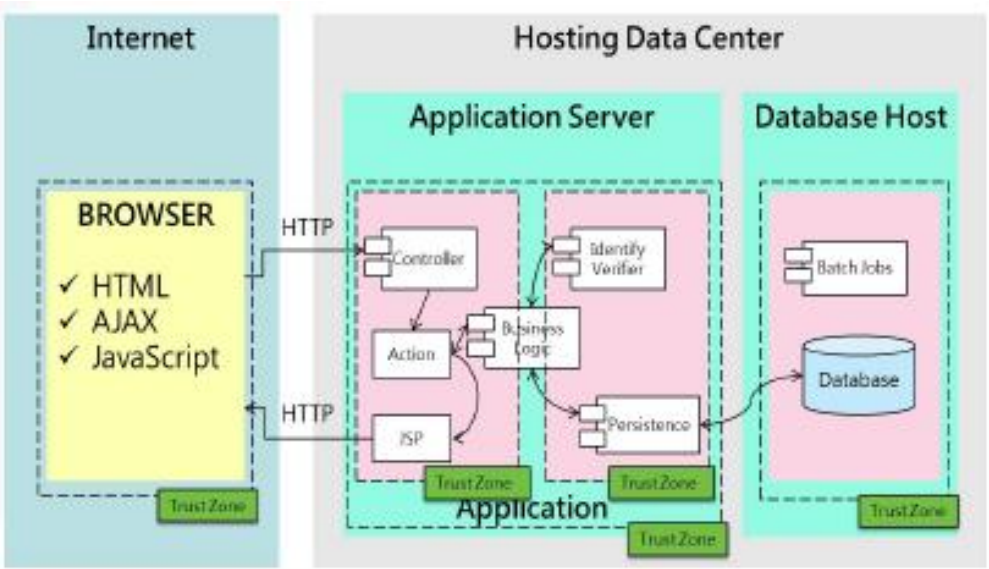
● 與「威脅建模」相似，但採用「已知」攻擊或弱點清單
– OWASP Top 10
– SANS Top 25
– WASC Attack & Weakness list

編號	攻擊
1	功能濫用(Abuse of Functionality)
2	暴力法攻擊(Brute Force)
3	緩衝區溢位(Buffer Overflow)
4	內容偽冒(Content Spoofing)
5	認證與會話神祕碼的預測(Credential/Session Prediction)
6	跨站腳本攻擊(Cross-Site Scripting, XSS)
7	跨站冒名請求(Cross-Site Request Forgery, CSRF)
8	阻絕服務(Denial of Service)
9	指紋探索與辨識(Fingerprinting)
10	格式化字串攻擊(Format String)
11	HTTP 回應偷渡(HTTP Response Smuggling)
12	HTTP 回應分割攻擊(HTTP Response Splitting)
13	HTTP 請求偷渡(HTTP Request Smuggling)
14	HTTP 請求分割攻擊(HTTP Request Splitting)
15	整數溢位(Integer Overflows)
16	LDAP 注入(LDAP Injection)
17	郵件命令注入(Mail Command Injection)
18	空字元注入(Null Byte Injection)
19	未經授權執行作業系統命令(OS Commanding)
20	路徑尋訪(Path Traversal)
21	可預測的資源位置(Predictable Resource Location)
22	遠端檔案含入(Remote File Inclusion, RFI)



模糊分析(Ambiguity Analysis)

- 用來發現新威脅的分析活動
- 需要兩組(位)以上對系統架構熟悉的人員
- 進行下列活動，然後比較其產出差異性，進行討論
  - 威脅建模
  - 敏感性資料建模



底層框架弱點分析 (Underlying Framework Weakness Analysis)

- 系統依賴其他底層軟體元件
- 底層軟體的安全問題影響系統安全
- 尋找底層軟體已知安全弱點

範例 –檢視底層軟體弱點

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-validator-1.3.1.jar	cpe:/a:apache:apache_http_server:1.3.1	commons-validator:commons-validator:1.3.1	Medium	2	LOW	22
httpclient-4.2.3.jar	cpe:/a:apache:httpclient:4.2.3	org.apache.httpcomponents:httpclient:4.2.3	Medium	1	HIGHEST	14
mail.jar	cpe:/a:sun:javamail:1.4.2	javax.mail:mail:1.4.2	Medium	1	LOW	15
poi-3.6-20091214.jar	cpe:/a:apache:poi:3.6	org.apache.poi:poi:3.6	Medium	4	HIGHEST	12
solr-core-4.2.0.jar	cpe:/a:apache:solr:4.2.0		Medium	3	HIGHEST	8
spring-2.5.jar	cpe:/a:springsource:spring_framework:2.5.0 cpe:/a:vmware:springsource_spring_framework:2.5		High	7	HIGHEST	12
spring-mock-2.0-m4.jar	cpe:/a:springsource:spring_framework:2.0:m4 cpe:/a:vmware:springsource_spring_framework:2.0.m4	org.springframework:spring-mock:2.0-m4	High	6	HIGHEST	15
standard.jar	cpe:/a:apache:standard_taglibs:1.1.2		High	1	LOW	6
struts2-core-2.3.16.3.jar	cpe:/a:apache:struts:2.3.16.3	org.apache.struts:struts2-core:2.3.16.3	Medium	2	HIGHEST	13
struts2-tiles-plugin-2.3.16.3.jar	cpe:/a:apache:struts:2.3.16.3 cpe:/a:apache:tiles:2.3.16.3	org.apache.struts:struts2-tiles-plugin:2.3.16.3	Medium	2	HIGHEST	14
xwork-core-2.3.16.3.jar	cpe:/a:apache:struts:2.3.16.3	org.apache.struts.xwork:xwork-core:2.3.16.3	Medium	2	HIGHEST	23

資通安全防護及控制措施

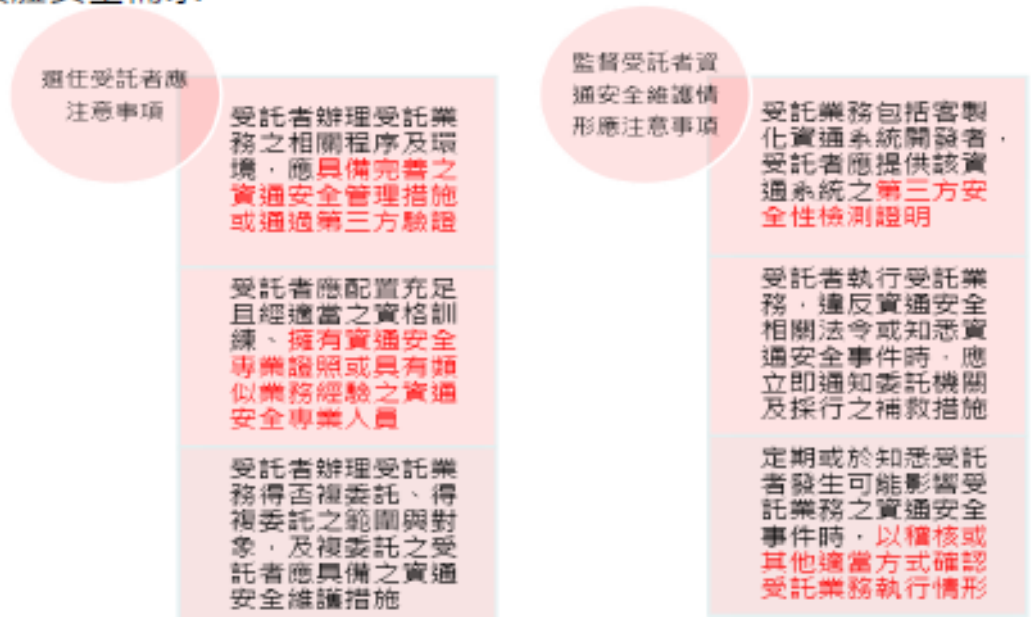
- **業務持續運作演練**(有核心資通系統之C級機關為例)
  - 應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練
- **執行資通安全健診**(C級機關為例)
  - 每二年應辦理資通安全健診，並檢討執行情形
    - 網路架構檢視
    - 網路惡意活動檢視
    - 使用者端電腦惡意活動檢視
    - 伺服器主機惡意活動檢視
    - 安全設定檢視

資通安全防護及控制措施

- 資通安全防護設備
  - 建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級
  - 資安設備定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形

資通系統或服務委外辦理之管理

- 依資安管理法施行細則第4條規定，委外辦理資通系統建置、維運或資通服務提供時，應考量受託者專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形
- 機關同仁辦理資訊作業委外時，可參考行政院國家資通安全會報頒布之最新「 政府資訊作業委外安全參考指引」，於資訊委外各階段，訂定具體安全需求



資通安全教育訓練

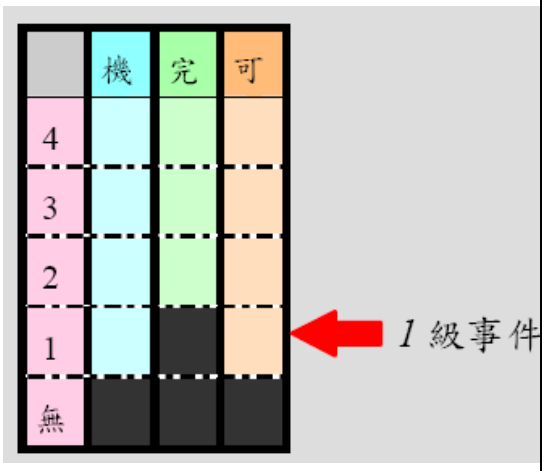
- **資通安全教育訓練要求**(以A級機關為例)
  - 依資通安全責任等級分級屬A級，資安及資訊人員每年至少4名人員接受12小時以上之資安專業課程訓練或資安職能訓練
  - 一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練
- 資通安全教育訓練辦理方式
  - 擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練之紀錄
  - 認知宣導及教育訓練之內容得包含
    - 資通安全政策
    - 資通安全法令規定
    - 資通安全作業內容
    - 資通安全技術訓練

Q & A

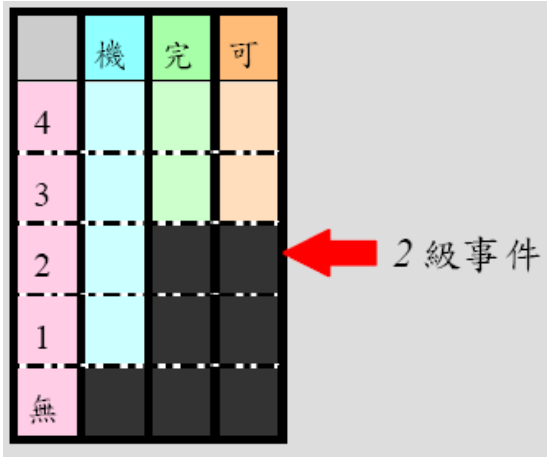

THE
END

附件二　資通安全處理小組演練劇本

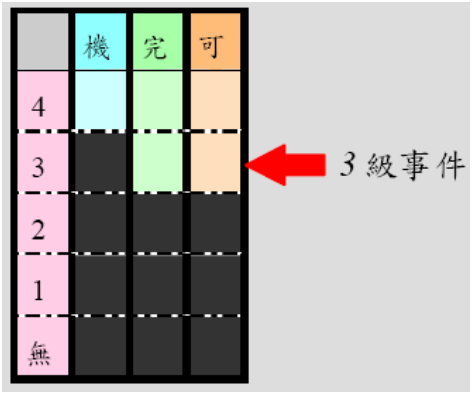
判定參考案例1（電腦中毒或被植入間諜軟體）

<table>
<tr><td>情境</td><td colspan="2">A 機關接獲技術服務中心入侵事件警訊，發現內部一名員工電腦中毒，對外進行攻擊行為。此電腦為平時該員工處理一般性業務使用，並無存放機敏性公務資料。A 機關資訊人員，針對受駭電腦進行解毒程序處理，原電腦的使用者則使用備用電腦繼續辦公。A機關資訊人員依通報應變作業規定登入通報應變網站進行通報作業。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性：因此次電腦中毒未造成資料外洩情形，選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 此電腦為一般性業務使用，但其系統已遭變更竄改，故選擇「1 級」。</td></tr>
<tr><td>可用性： 因此次電腦中毒並無影響平常工作業務，故選擇「無需通報」。</td></tr>
<tr><td>綜合評估</td><td>因第二項目為「1 級事件」，第一、三項目為「無需通報」，故綜合評估此資安事件為「1 級事件」。</td><td></td></tr>
</table>

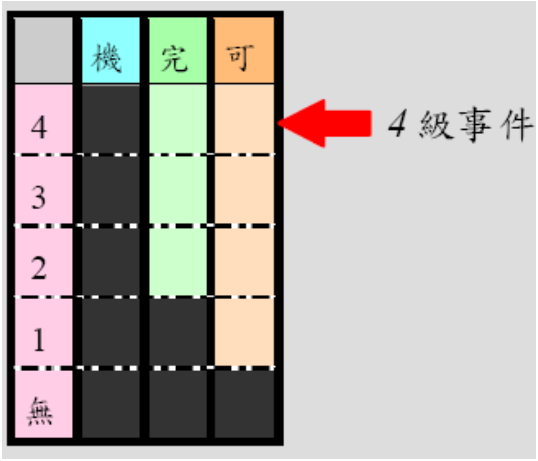
判定參考案例2（電腦中毒或被植入間諜軟體）

<table>
<tr><td>情境</td><td colspan="2">B 機關有100 台電腦中毒，其中有5 台電腦存有核心業務資料。這種病毒僅會將電腦硬碟內資料刪除，估計共有100 台電腦資料遭刪除，核心業務因此也受到影響。透過解毒程序處理後，系統已於3 小時後完全恢復，遭病毒刪除資料亦已救回。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 電腦存放資料雖遭刪除，但並未洩漏出去，故選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 因電腦資料已遭刪除，且刪除資料為核心業務資料，經B 機關自行判斷後認定資料遭刪除情形屬輕微，故選擇「2 級」。</td></tr>
<tr><td>可用性： 因此次電腦中毒事件造成核心業務中斷3 小時，經通報單位自行判斷後，判定為在可容忍時間內恢復正常運作，故選擇「2 級」。</td></tr>
<tr><td>綜合評估</td><td>因第一項目為「無需通報」，但第二、三項目為「2 級」，故綜合評估此資安事件為「2 級事件」。</td><td></td></tr>
</table>

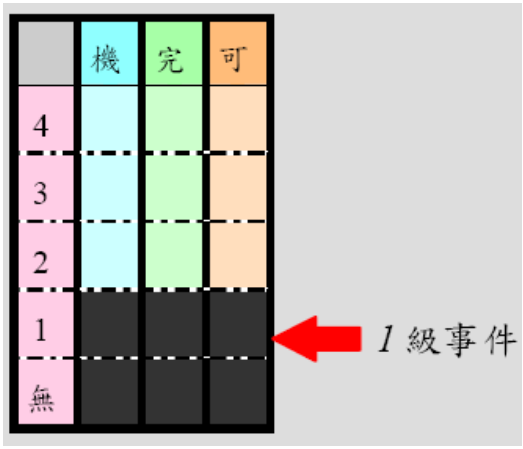
判定參考案例3（電腦中毒或被植入間諜軟體）

<table>
<tr><td>情境</td><td colspan="2">C 機關有100 台電腦中毒，其中首長及其幕僚使用的電腦亦遭感染，檔案伺服器似乎也遭感染。部份員工及首長等人所使用之電腦中，有存放核心業務資料。經檢測病毒後研判為USB 隨身碟病毒，此病毒會感染USB 隨身碟，及其他插入受感染USB 隨身碟的電腦，並會將遭感染電腦的檔案，透過網路上傳至駭客電腦，因此評估至少已有多筆機敏資料遭竊取。透過解毒程序處理後，中毒系統已於2 小時後完全恢復。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性：經查網路連線後，發現電腦存放資料已遭洩漏，其中包含敏感及密級公務資料，故選擇「3級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性：因這種病毒僅對中毒電腦進行系統竄改，並無對公務資料進行竄改，且一般公務電腦應無運作核心業務，在此情形下，系統中毒時應選擇「1級」。但此情境中描述檔案伺服器亦遭感染中毒，由於伺服器通常會搭配運作核心業務，故判定此情形為核心業務系統遭病毒輕微竄改系統檔案，選擇「2級」。綜合此兩點判斷，應將完整性所造成的衝擊影響選為「2 級」。</td></tr>
<tr><td>可用性：因電腦中毒後，共花費2 小時進行解毒程序，經通報單位自行判斷後，判定為在可容忍時間內恢復正常運作，故選擇「2級」。</td></tr>
<tr><td>綜合評估</td><td>因第一項目為「3 級」，第二、三項目為「2 級」，故綜合評估此資安事件為「3 級事件」。</td><td></td></tr>
</table>

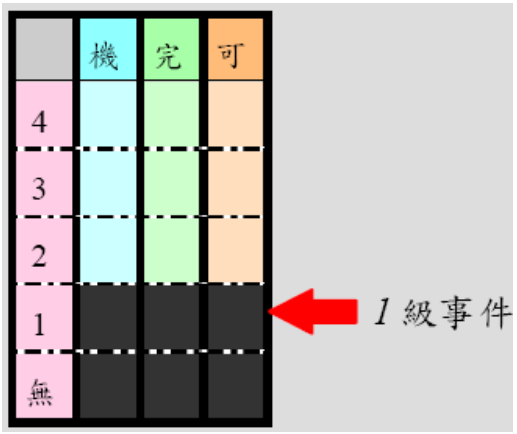
判定參考案例4（電腦中毒或被植入間諜軟體）

<table>
<tr><td>情境</td><td colspan="2">D 機關有10 台電腦中毒，其中首長及其幕僚使用的電腦亦遭感染。經檢測病毒後研判為USB 隨身碟病毒，此病毒會感染USB 隨身碟，及其他插入受感染USB 隨身碟的電腦，並會將遭感染電腦的檔案，透過網路上傳至駭客電腦，因此評估至少已有多筆機敏資料遭竊取，其中甚致包含國家機敏資料。經重新安裝電腦系統後，始解除中毒情形，原電腦的使用者則使用備用電腦繼續辦公。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 經查網路連線後，發現電腦存放資料已遭洩漏，其中包含國家機密資料，故選擇「4 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 因這種病毒僅對中毒電腦進行系統竄改，並無對公務資料內容進行竄改，且一般公務電腦應無運作核心業務，在此情形下，系統中毒時應選擇「1級」。</td></tr>
<tr><td>可用性： 電腦中毒後，需等待電腦系統重新安裝，但因該單位有備用電腦可供使用，故選擇「無需通報」。</td></tr>
<tr><td>綜合評估</td><td>因第一項目為「4 級」，第二項目為「1 級」，第三項目為「無需通報」，故綜合評估此資安事件為「4級事件」。</td><td></td></tr>
</table>

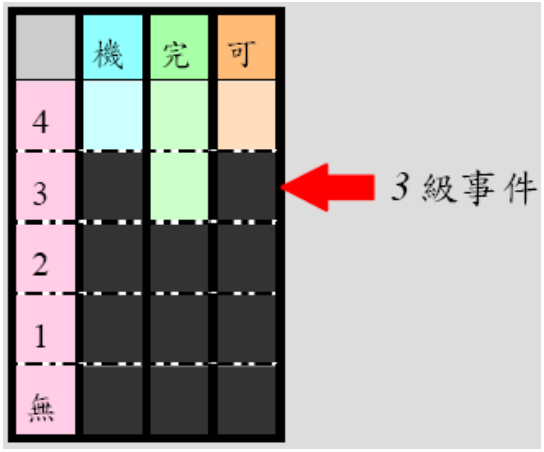
判定參考案例5（網頁遭置換或竄改）

<table>
<tr><td>情境</td><td colspan="2">E 機關網站主機遭駭客入侵，並將網站首頁置換為惡意網頁，網站主機內有存放一般公務用資料，網站主機主要用途是放置單位形象網頁。E 機關人員一發現網站遭置換後，馬上將網站備份程式復原至網站主機，同時進行全面系統檢測。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 由於網站主機遭入侵，一般公務資料可能已遭洩漏，故選擇「1 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 網站主機首頁被置換為惡意網頁，且網站主機主要用途是放置單位形象網頁，並無用來執行或運作其他核心業務，故判定為非核心業務系統遭竄改，選擇「1 級」。</td></tr>
<tr><td>可用性： 形象網站非屬E 機關核心業務，故選擇「1 級」。</td></tr>
<tr><td>綜合評估</td><td>因三項目均為「1 級」，故綜合評估此資安事件為「1 級事件」。</td><td></td></tr>
</table>

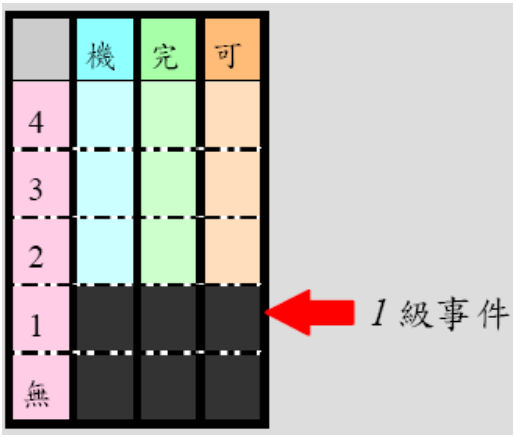
判定參考案例6（網頁遭置換或竄改）

<table>
<tr><td>情境</td><td colspan="2">F 機關主機遭駭客入侵，並在網站首頁檔案中植入一段惡意程式碼「<iframe src=http://xxxxxxx」，導致來瀏覽此網頁的民眾皆反應疑似中毒。網站主機內有存放一般公務用資料，主要用途是放置單位形象網頁。F 機關人員一發現網站遭竄改後，馬上將受駭網站關閉，並啟動備援系統恢復網站服務運作。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 由於網站主機遭入侵，一般公務資料可能已遭洩漏，故選擇「1 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 網站主機首頁被植入為惡意程式碼，且網站主機主要用途是放置單位形象網頁，並無用來執行或運作其他核心業務，故判定為非核心業務系統遭竄改，選擇「1 級」。</td></tr>
<tr><td>可用性： 形象網站非屬F 機關核心業務，故選擇「1 級」。</td></tr>
<tr><td>綜合評估</td><td>因三項目均為「1 級」，故綜合評估此資安事件為「1 級事件」。</td><td></td></tr>
</table>

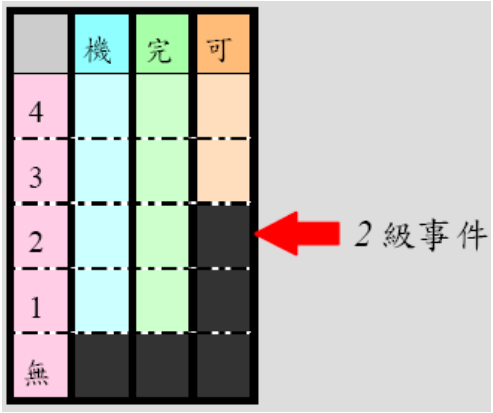
判定參考案例7（網頁遭置換或竄改）

<table>
<tr><td>情境</td><td colspan="2">G 機關網站主機遭駭客入侵，並修改網站首頁內容。網站主機內有存放一般公務用資料及民眾個人資料。在發現網站遭修改後，G 機關立即將網頁首頁檔案修正還原，並將系統暫時停止服務1 日，以檢查網站是否有安全漏洞未修補，或遭駭客植入後門程式。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 由於網站主機遭入侵，民眾個人資料可能已遭洩漏，已危害民眾個人之權益，故選擇「3 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 因網站主機負責該機關主要業務系統，故核心業務系統可能已遭竄改，需視系統或資料被竄改情形選擇「2 級」或「3 級」。假設此情境經該單位檢查後判定僅遭輕微竄改，則選擇「2 級」。</td></tr>
<tr><td>可用性： 由於需將網站服務停止1日，經判定超過可容忍中斷時間，故選擇「3 級」。</td></tr>
<tr><td>綜合評估</td><td colspan="2">因第一項目皆為「3 級」，第二項目為「2 級」，第三項目為「3 級」，故綜合評估此資安事件為「3 級事件」。</td></tr>
</table>

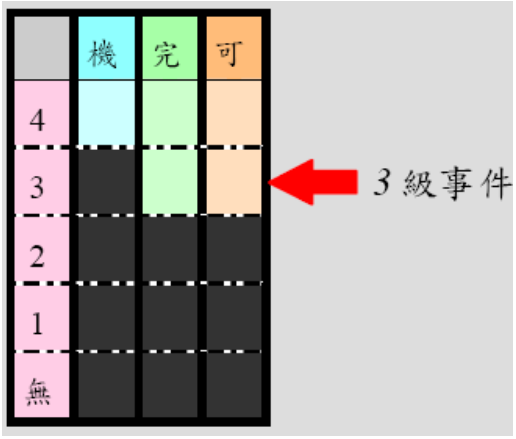
判定參考案例8（網頁遭置換或竄改）

<table>
<tr><td>情境</td><td colspan="2">H 機關網主機遭駭客入侵，並在其網站主機上架設詐騙網站，試圖詐騙一般民眾。網站主機內有僅存放一般公務用資料。H 機關資訊人員一發現網站主機遭駭客利用架設詐騙網站後，馬上將該詐騙網頁移除，並將系統暫停服務2 日，進行系統檢查。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 由於網站主機遭入侵，一般公務資料可能已遭洩漏，故選擇「1 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 雖然網站主機遭駭客利用架設詐騙網站，但網站主機僅用來放置H 機關形象網頁，並無用來執行或運作其他核心業務，故判定為非核心業務系統遭竄改，選擇「1 級」。</td></tr>
<tr><td>可用性： 由於網站雖停止服務2 日，但因網站提供服務並非核心業務，故判定為非核心業務受影響，選擇「1 級」。</td></tr>
<tr><td>綜合評估</td><td>因三項目皆為「1 級」，故綜合評估此資安事件為「1 級事件」。</td><td></td></tr>
</table>

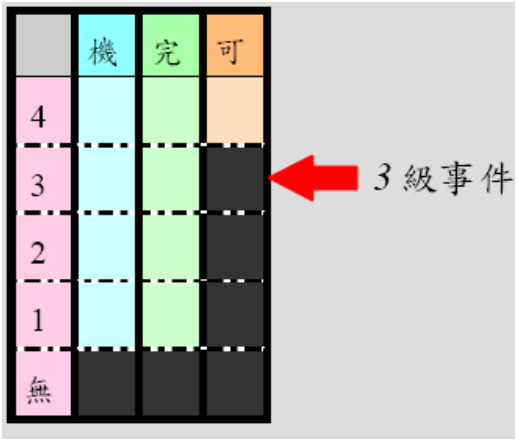
判定參考案例9（網站遭受阻斷式服務攻擊(Denial of Service Attack)）

<table>
<tr><td>情境</td><td colspan="2">I 機關資訊人員發現民眾反應時常無法開啟I 機關網頁。經查詢系統Log 檔及防火牆Log檔紀錄後，發現有數個IP 正對網站伺服器送出大量的連線請求，導致I 機關網路對外頻寬幾乎滿載，一般民眾無法連上網頁查詢資料及辦理網路便民服務。</td></tr>
<tr><td rowspan="4">解析</td><td>機密性： 因此次阻斷式服務攻擊僅造成民眾無法連上I機關網站，並無造成任何資料遭洩漏，故選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 因此次阻斷式服務攻擊僅造成民眾無法連上I機關網站，並無造成任何資料遭竄改，故選擇「無需通報」。</td></tr>
<tr><td>可用性： 阻斷式服務攻擊僅造成民眾無法連上I 機關網站，使得網站提供的服務無法運作。評定分級時，應依照該網站提供之服務來做判斷，若網站主機僅放置單位形象網頁，選擇「1 級」；網站主機除放置單位形象網頁，還提供便民服務業務或其他業務，則視是否於可容忍中斷時間內回復正常運作，選擇「2 級」或「3 級」。假設此次事件導致網路便民服務業務中斷3 小時，I 機關認定中斷時間在可容忍範圍內，則應選擇「2 級」。</td></tr>
<tr><td>綜合評估</td><td colspan="2">因第一、二項目為「無需通報」，第三項目為「2 級」，故綜合評估此資安事件為「2 級事件」。</td></tr>
</table>

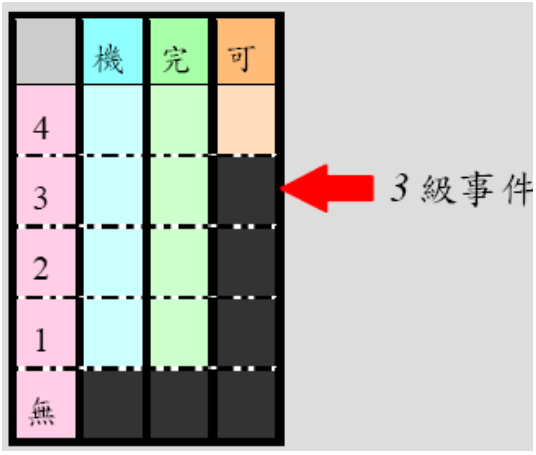
判定參考案例10（電腦對外攻擊）

<table>
<tr><td>情境</td><td colspan="2">J 機關收到技術服務中心所發出的入侵事件警訊，表示J 機關的某台機器正在對外攻擊。經網管人員檢查後，發現該台機器為一檔案伺服器，存放有單位核心業務所需資料及部分敏感公務資料，並如通告所言，正在對外進行網路攻擊。網管人員同時發現該機器系統設定遭到變動，故將該機器重新安裝系統，共計停止服務4 小時。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性：受影響的機器若無公務資料遭洩漏，則選擇「無需通報」；若存放之一般公務資料遭洩漏，則需選擇「1 級」。但此情境中受影響的為一檔案伺服器，內含有部份敏感公務資料，故當有資料遭竊疑慮時，則需選擇「3 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性：J 機關判斷該伺服器為核心業務系統，且系統設定已遭變更，故遭駭客利用對外發動攻擊，但由於檔案資料未遭變更，認定竄改情形輕微，故選擇「2 級」。</td></tr>
<tr><td>可用性：由於伺服器提供服務為核心業務且停止服務4小時，判定為可容忍中斷時間，故選擇「2 級」。</td></tr>
<tr><td>綜合評估</td><td>因第一項目為「3 級」，第二、三項目為「2 級」，故綜合評估此資安事件為「3 級事件」。</td><td></td></tr>
</table>

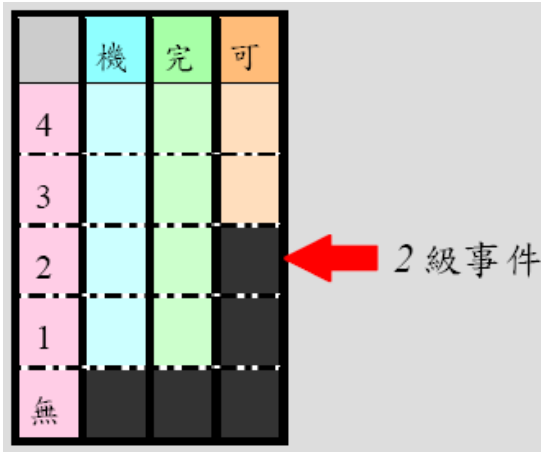
判定參考案例11（網路、資訊設備故障）

<table>
<tr><td>情境</td><td colspan="2">K 機關網站主機，因網路設備故障，導致K 機關網路服務中斷。經聯繫廠商更換網路機房設備後，始於5 小時後恢復對外正常網路連線。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性：因無任何資料遭洩漏，選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性：因無任何資料遭竄改，選擇「無需通報」。</td></tr>
<tr><td>可用性：K 機關認定網路服務為核心業務，此事件造成核心業務中斷5 小時，K 機關認定已超過可容忍中斷時間，故選擇「3 級」。</td></tr>
<tr><td>綜合評估</td><td>因第一、二項目為「無需通報」，第三項目為「3 級」，故綜合評估此資安事件為「3 級事件」。</td><td></td></tr>
</table>

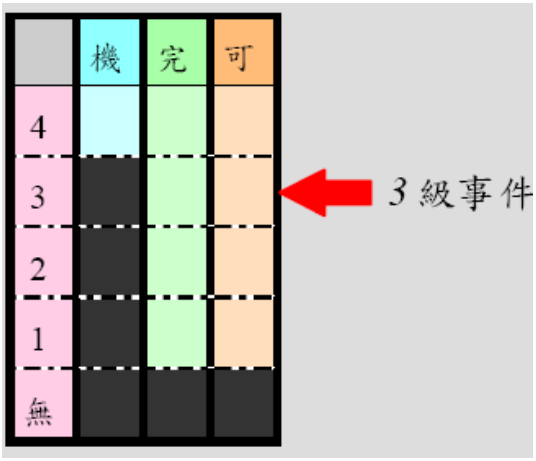
判定參考案例12（網路、資訊設備故障）

<table>
<tr><td>情境</td><td colspan="2">L 機關網站檔案服器因硬碟壞軌，導致無法正常存取辦公文件。經聯繫廠商更換硬碟設備後，始於6 小時後恢復正常資料存取，但檢查後發現大部分核心業務使用之檔案毀損無法開啟，且無檔案備份機制來備份這些核心業務使用檔案，評估若要將損毀資料復原則至少需5 日。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 因硬碟故障導致無法存取辦公文件，並無任何資料遭洩漏，故選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 由於硬碟為正常使用下故障，其內容未遭竄改，故選擇「無需通報」。</td></tr>
<tr><td>可用性： 因硬碟故障導致部分辦公文件損毀，在更換新設備後，發現已有部分檔案毀損無法開啟，造成核心業務資料無法取得，同時又無檔案備份機制來復原核心業務資料，造成使用者無法存取核心業務所需資料。經L 機關自行判定6 小時超過可容忍中斷時間，且損毀資料復原評估至少需5日，故選擇「3 級」。</td></tr>
<tr><td>綜合評估</td><td colspan="2">因第一、二項目為「無需通報」，第三項目為「3 級」，故綜合評估此資安事件為「3 級事件」。</td></tr>
</table>

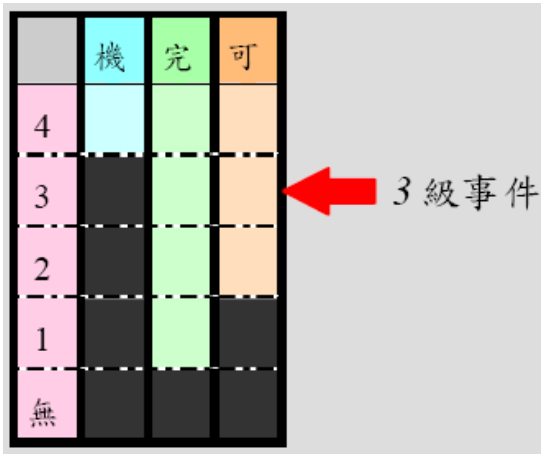
判定參考案例13（網路、資訊設備故障）

<table>
<tr><td>情境</td><td colspan="2">XX 縣某區域變電箱遭人蓄意破壞，導致XX 縣該區暫時停止供電5 小時，連帶使得位在該區域的M 機關業務全面中斷5 小時。M 機關打算對此進行資安事件通報。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 因變電箱遭人破壞，使得M 機關業務中斷5 小時，此事件並無造成M 機關有任何資料遭洩漏，故選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 因變電箱遭人破壞，使得M 機關業務中斷5 小時，此事件並無造成M 機關任何資料遭竄改，故選擇「無需通報」。</td></tr>
<tr><td>可用性： 對M 機關來說，因變電箱遭人破壞，業務全面中斷5 小時，經M 機關自行認定5 小時為可容忍中斷時間，故選擇「2 級」。</td></tr>
<tr><td>綜合評估</td><td colspan="2">因第一、二項目為「無需通報」，第三項目為「2 級」，故綜合評估此資安事件為「2 級事件」。</td></tr>
</table>

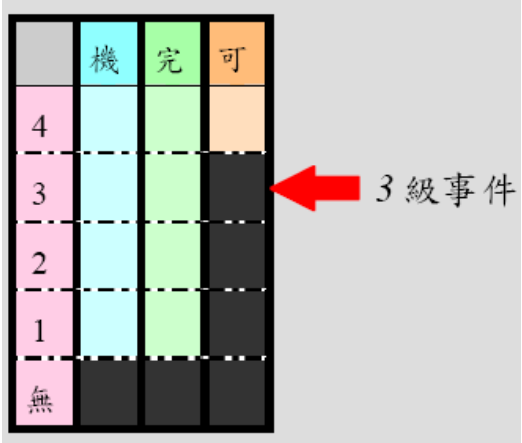
判定參考案例14（業務資料外洩）

<table>
<tr><td>情境</td><td colspan="2">N 機關舉辦終身學習課程，N 機關人員將參與課程的民眾個人資料，包含姓名、電話、住址、身分證字號等資訊公布於網站主機上供民眾下載。在民眾告知此事情後，N 機關資訊人員已在第一時間將民眾資料自網站取下。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性：此事件已民眾個人資料外洩，危害民眾個人之權益，故選擇「3 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性:此事件並無造成系統或資料遭竄改，故選擇「無需通報」。</td></tr>
<tr><td>可用性:此事件並無造成N 機關業務受影響，故選擇「無需通報」。</td></tr>
<tr><td>綜合評估</td><td>因第一項目為「3 級」，第二、三項目為「無需通報」，故綜合評估此資安事件為「3 級事件」。</td><td></td></tr>
</table>

判定參考案例15（業務資料外洩）

<table>
<tr><td>情境</td><td colspan="2">0 機關員工，於工作電腦安裝p2p 軟體，又未將軟體做適當設定，導致工作業務資料遭其他p2p 使用者下載，其中更包含民眾的個人資料文件。在發現此情形後資訊人員已將電腦系統重新安裝，並於1 日後歸還該員工繼續使用。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 此資安事件已將執行業務相關的民眾個人資料外洩，危害民眾個人之權益，故選擇「3 級」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 因p2p 軟體並未對系統或資料進行竄改，資料外洩乃因軟體設定不當所造成，選擇「無需通報」。</td></tr>
<tr><td>可用性： 因電腦系統重新安裝，並於1 日後才取得可用電腦，導致該員工無法正常執行業務。但由於安裝p2p 軟體之電腦為工作使用之個人電腦，並非工作伺服器，故判定僅非核心業務運作遭影響，選擇「1 級」。</td></tr>
<tr><td>綜合評估</td><td colspan="2">因第一項目為「3 級」，第二項目為「無需通報」，第三項目為「1 級」，故綜合評估此資安事件為「3 級事件」。</td></tr>
</table>

判定參考案例16（天災）

<table>
<tr><td>情境</td><td colspan="2">因颱風來襲，導致全台多處淹水，P 機關也因颱風導致地下室機房淹水、對外網路全面中斷、伺服器故障、硬碟資料毀損、業務無法運行。專家評估仍需三星期才能恢復網路基本運作，硬碟毀損資料需7 日才可救回。P 機關打算對此進行資安事件通報。</td></tr>
<tr><td rowspan="3">解析</td><td>機密性： 因淹水並無導致任何資料遭洩漏，故選擇「無需通報」。</td><td rowspan="3"> 
</td></tr>
<tr><td>完整性： 由於淹水導致P 機關地下室機房眾多電腦設備故障，內含資料亦遭毀損，但資料毀損為不可抗拒天災所造成，並非經由他人透過非授權方式損毀，故選擇「無需通報」。</td></tr>
<tr><td>可用性： 因專家評估設備修復至少仍需三星期才可恢復基本運作，硬碟毀損資料需7 日才可救回，經P機關評估認定為無法於可容忍中斷時間內恢復正常運作，故選擇「3 級」。</td></tr>
<tr><td>綜合評估</td><td colspan="2">因第一、二項目為「無需通報」，第三項目為「3 級」，故綜合評估此資安事件為「3 級事件」。</td></tr>
</table>