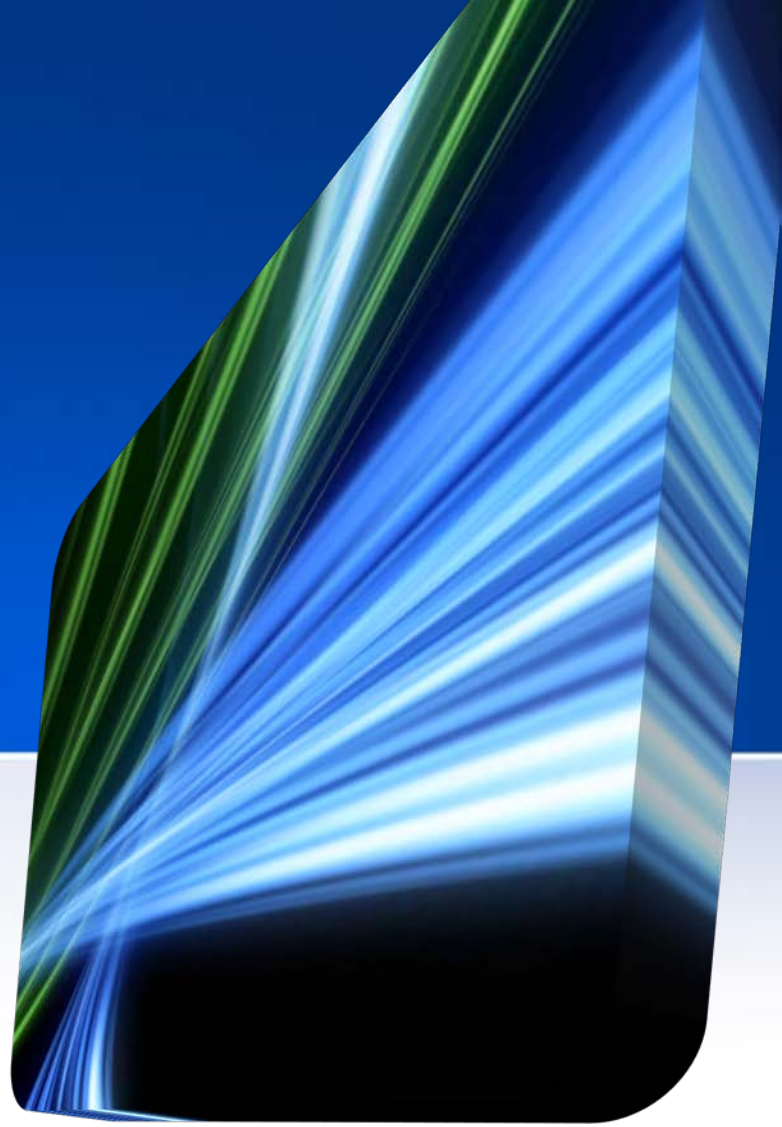
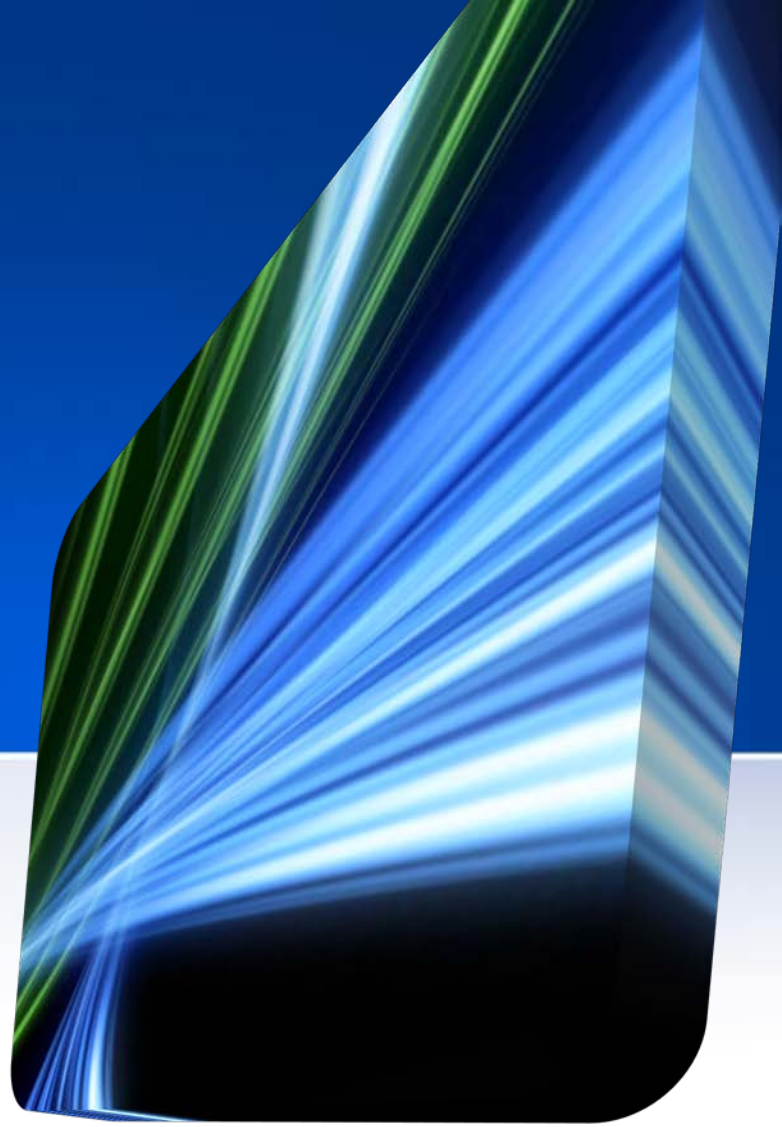
資通安全管理法之簡介
及
連線單位面對資安法之
應因建議淺見





資通安全管理法之簡介

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

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

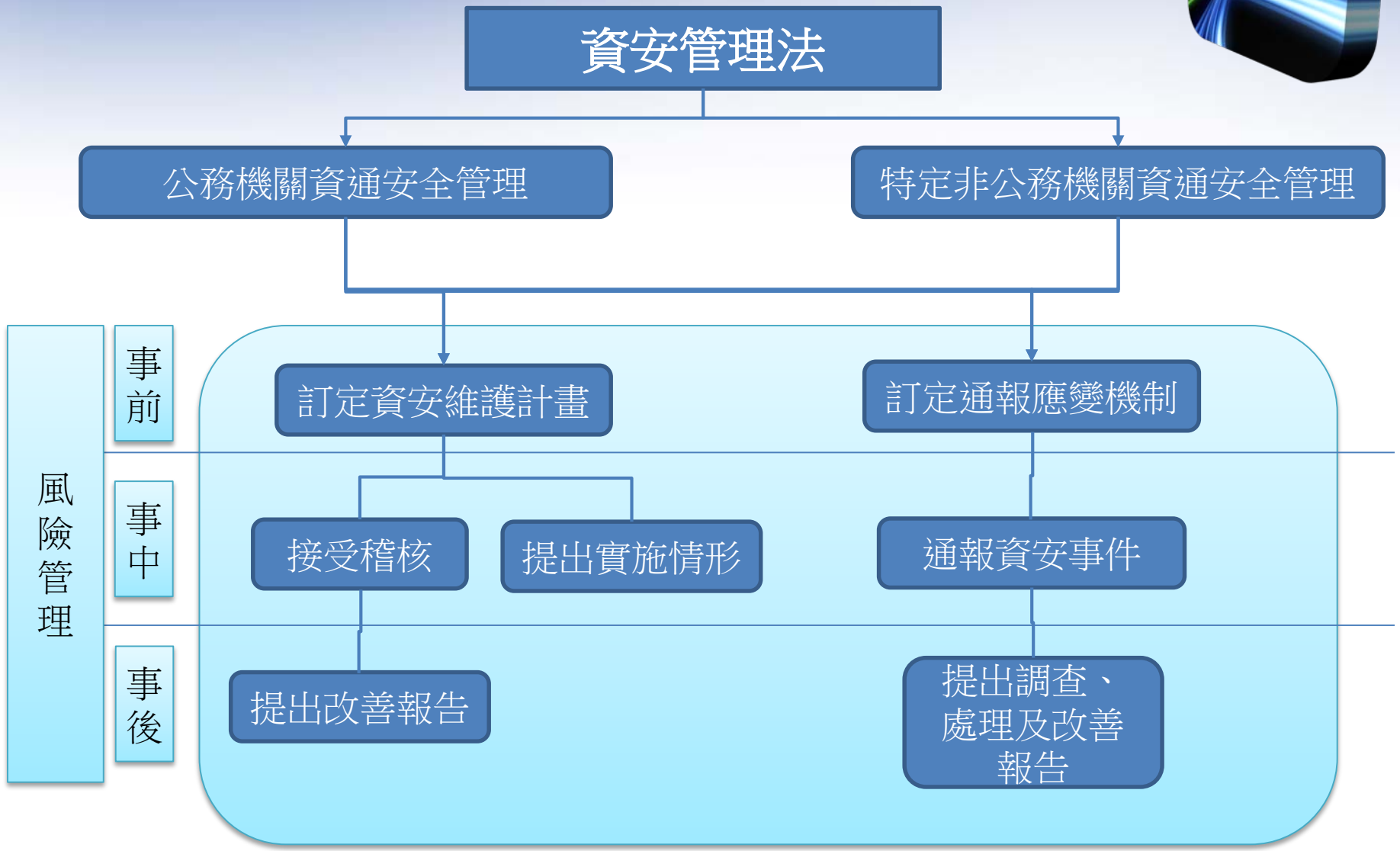
- 資安管理法第3條第5款
  公務機關：指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。

- 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)

資安法架構


資安管理法
公務機關資通安全管理
特定非公務機關資通安全管理
風險管理
事前
事中
事後
訂定資安維護計畫
訂定通報應變機制
接受稽核
提出實施情形
通報資安事件
提出改善報告
提出調查、處理及改善報告

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

資安管理法子法架構

- 機關資安責任等級分級提報
- 制定資安維護計畫

規劃

運作

- 提出資安維護計畫實施情形
- 進行稽核

改善

通報

- 提出稽核改善報告
- 情資分享
- 人員獎懲

- 制定資安事件通報應變機制
- 通報資安事件

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

責任等級分級原則

國家機密、涉及外交、國防、國土安全事項

持有民眾或公務員個人資料檔案

公務機關涉及能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項

關鍵基礎設施服務，對社會公共利益、民心士氣，或民眾生命、身體、財產之影響

資通系統服務民眾之範圍

跨公務機關共用性資通系統之服務範圍

醫院分級

A級

B級

C級

D級

E級

資安責任等級

符合二個以上之資通安全責任等級者，列為其符合之最高等級

分級辦法

- 等級調整
  - 公務機關提交或核定資通安全責任等級時，得考量對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級
- 等級核定
  - 行政院直屬機關、提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，備文報主管機關核定
- 提報時機
  - 本法通過當年提報完整資料後，應每二年再行提報完整資料
  - 組織或業務調整，致須變更原資通安全責任等級時
- 提報執行情形
  - 公務機關之資通安全責任等級為A級或B級者，應依主管機關指定之方式，提報應辦事項之辦理情形

應辦事項

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

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	

應辦事項

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	1年內	1年內	

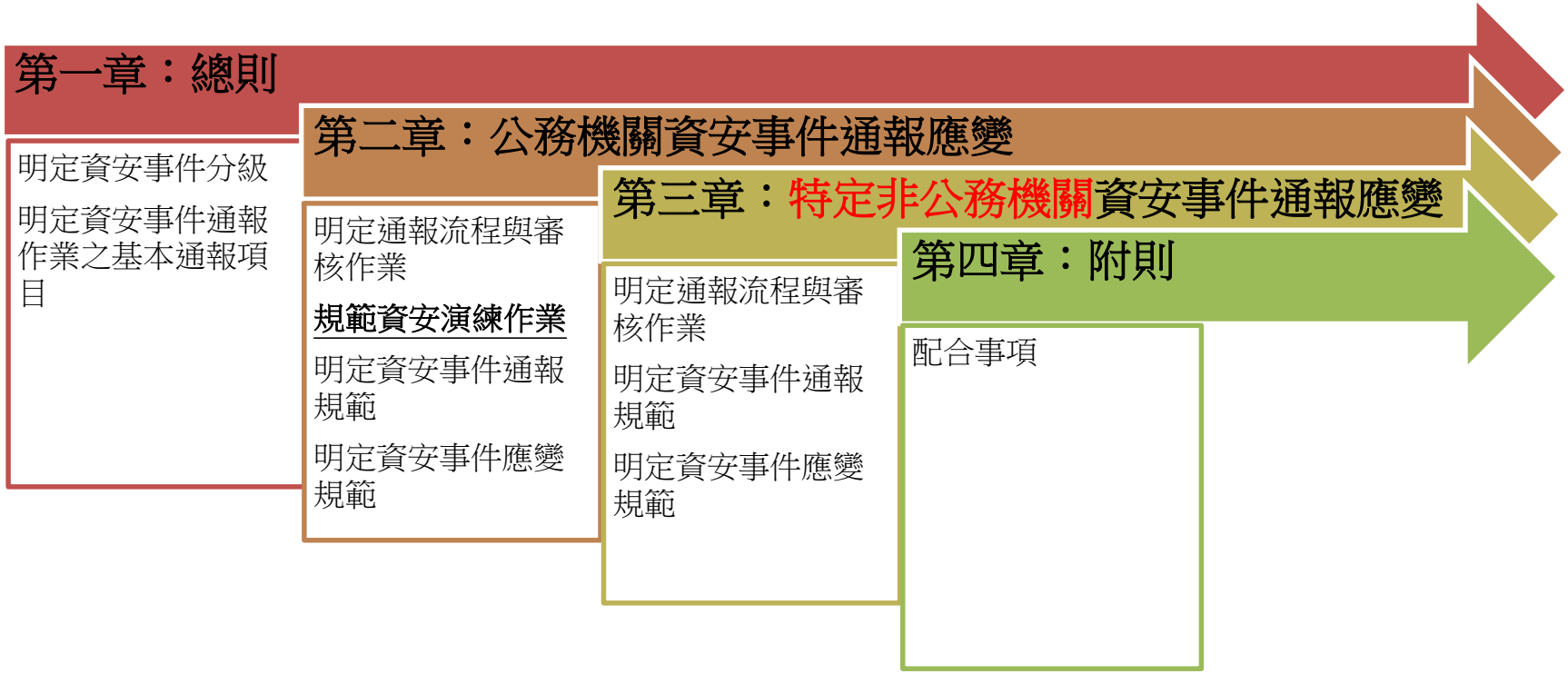
應辦事項

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

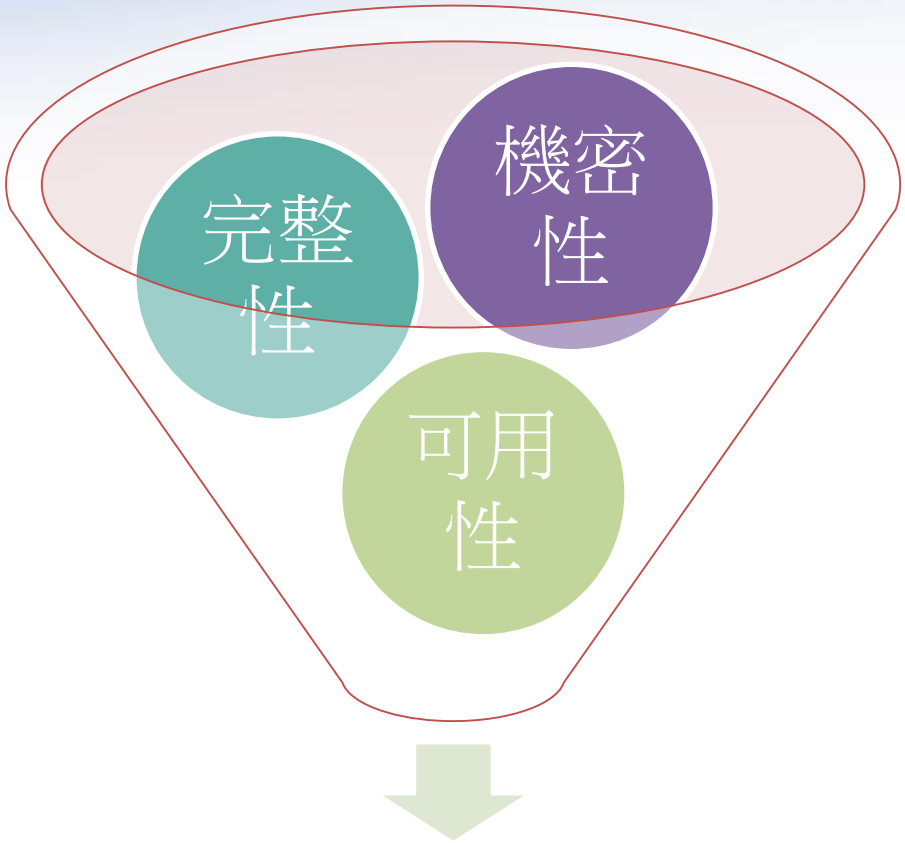
資通安全管理法

- 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

- 資通安全事件係指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅



資安事件等級判定方法 - 質化判定

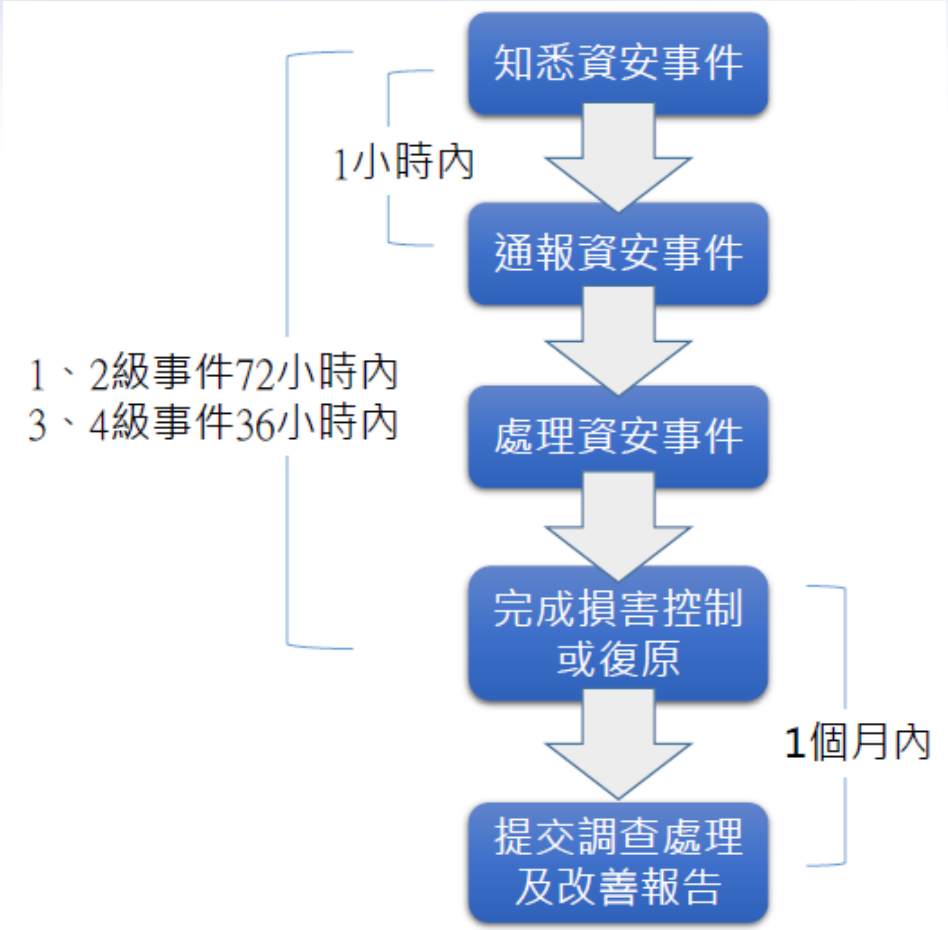


資安事件等級判定

資安事件等級綜合評估表

	機密性 資訊洩漏		完整性 資訊/資通系統遭竄改		可用性 業務/資通系統運作遭中斷	
	資訊性質	影響程度	業務資訊/資通系統	影響程度	業務/資通系統	可否於可容忍中斷時間回復
1級	非核心業務	輕微	非核心	輕微	非核心	可
2級	非核心業務	嚴重	非核心	嚴重	非核心	不可
	核心業務(未涉及CI維運)	輕微	核心(未涉及CI維運)	輕微	核心(未涉及CI維運)	可
3級	核心業務(未涉及CI維運)	嚴重	核心(未涉及CI維運)	嚴重	核心(未涉及CI維運)	不可
	核心業務(涉及CI維運)	輕微	核心(涉及CI維運)	輕微	核心(涉及CI維運)	可
	一般公務機密、敏感資訊	輕微	一般公務機密、敏感資訊	輕微		
4級	核心業務(涉及CI維運)	嚴重	核心(涉及CI維運)	嚴重	核心(涉及CI維運)	不可
	一般公務機密、敏感資訊	嚴重	一般公務機密、敏感資訊	嚴重		
	國家機密	-	國家機密	-		

通報作業流程各項目時限



- 上級/監督機關或中央目的事業主管機關接獲資安事件通報後，應於時限內進行審核作業，並視情況提供必要支援服務
  - 1、2級事件應於8小時內完成審核，3、4級事件應於2小時內完成審核
  - 中央目的事業主管機關須定期彙送1、2級資安事件

資安事件通報與應變規範

	資安事件通報作業	資安事件應變作業
目的	知悉資安事件發生時，迅速依作業規範執行通報作業，並確保相關人員熟悉作業流程	發生資安事件時，可依作業規範保留必要事件紀錄，防止災情擴大，並釐清事件發生經過
規範事項	◘ 判定事件等級之流程及權責 ◘ 事件之影響範圍、損害程度及機關因應能力之評估 ◘ 資通安全事件之內部通報流程 ◘ 通知受資通安全事件影響之其他機關之方式 ◘ 前四款事項之演練 ◘ 資通安全事件通報窗口及聯繫方式 ◘ 其他資通安全事件通報相關事項	◘ 應變小組之組織 ◘ 事件發生前之演練作業 ◘ 事件發生時之損害控制機制 ◘ 事件發生後之復原、鑑識、調查及改善機制 ◘ 事件相關紀錄之保全 ◘ 其他資通安全事件應變相關事項

資安作業彙整表

項目	內容
通報作業流程	於時限內完成「事件通報作業」、「損害控制」及「調查、處理及改善報告」作業
制定資安規範	• 訂定資安事件之通報作業規範 • 訂定資安事件之應變作業規範
事件通報對象	上級/監督機關、主管機關
配合上級/監督機關資安演練	• 社交工程演練每半年一次 • 資安事件通報演練每年一次
配合主管機關資安演練作業	• 社交工程演練 • 資安事件通報及應變演練 • 網路攻防演練 • 情境演練 • 其他必要之演練

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

特定非公務機關資通安全維護計畫實施情形稽核辦法

第一條
- 授權依據

第二條
- 本辦法之書面
- 得以電子文件為之

第三條
- 主管機關擇定當年受稽單位的考量因素、稽合計畫

第四條
- 辦理稽核之通知

第五條
- 受稽單位應配合事項

第六條
- 稽核小組的利益迴避及保密義務

第七條
- 稽核報告內容
- 報告交付時程

第八條
- 改善報告
- 執行情形
- 提出方式、時程

第九條
- 得要求受稽核機關之中央目的事業主管協助稽核作業

第十條
- 施行日期

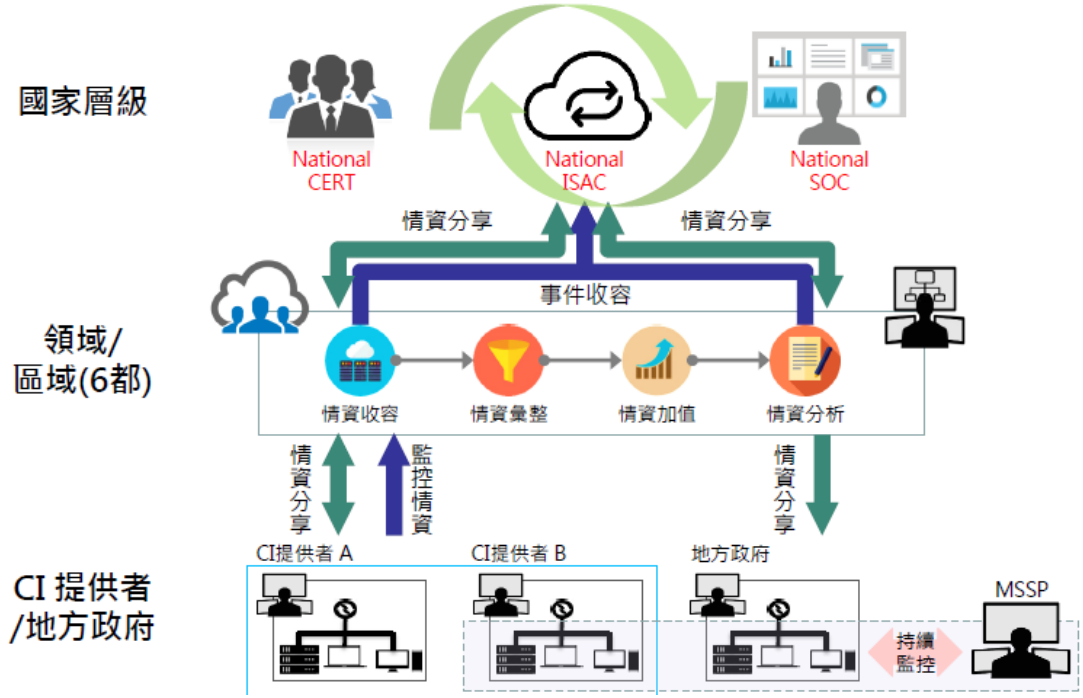
資通安全管理法

- 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

法源依據

- 資通安全管理法 (第8條)
  - 主管機關應建立資通安全情資分享機制
  - 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之

各層級情資分享架構



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

公務機關所屬人員資通安全事項獎懲辦法

第一條
- 授權依據

第二條
- 得自行訂定獎懲基準

第三條
- 明定應予獎勵之情形

第四條
- 明定應予懲處之情形

第五條
- 獎懲情形應納為考核評價。

第六條
- 懲處前，應給予當事人申辯之機會

第七條
- 施行日期

資安處 - 施行時程規劃

主管機關

11月上旬
- 發佈子法
- 函發整備函

12月上旬
- 提供範本文件

107年 | 108年 | 109年

11/09 | 11/30 | 12/07 | 02/28 | 03/31 | 01/30

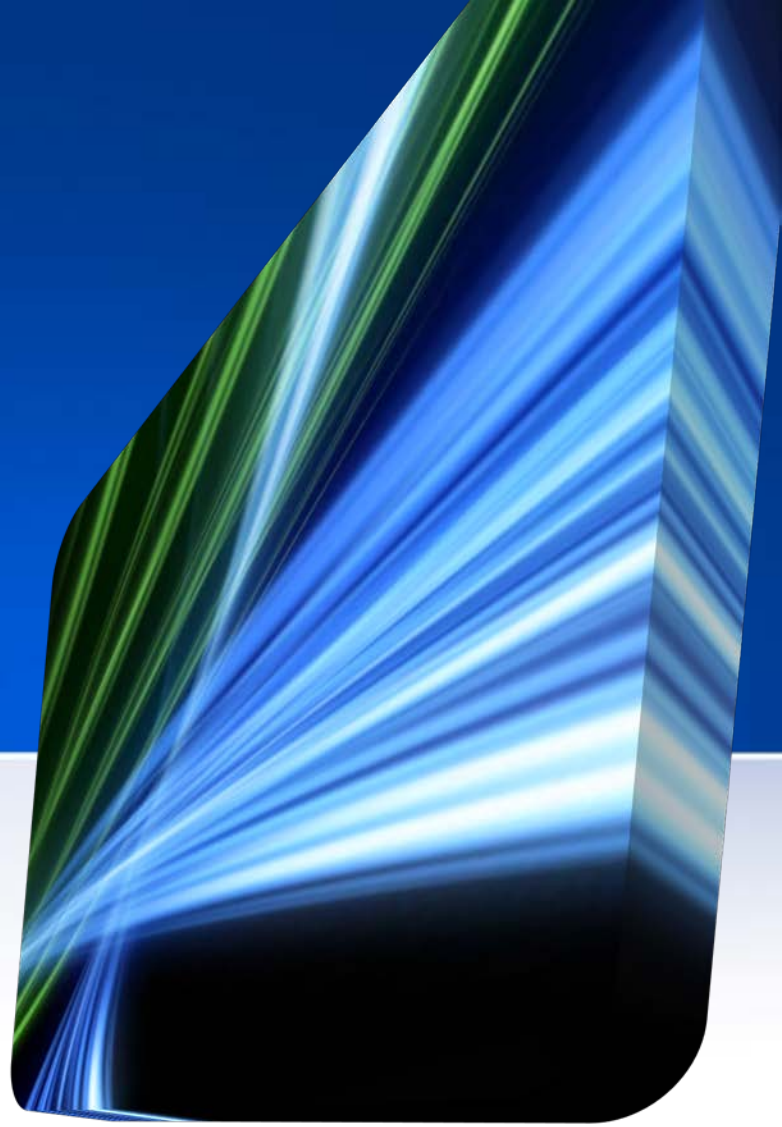
各機關

12月上旬
- 提報自身及所屬資通安全責任等級分級

2月下旬
- 提報公務機關維護計畫
- 提報事件通報應變程序
- 提報資產盤點及風險評鑑清單

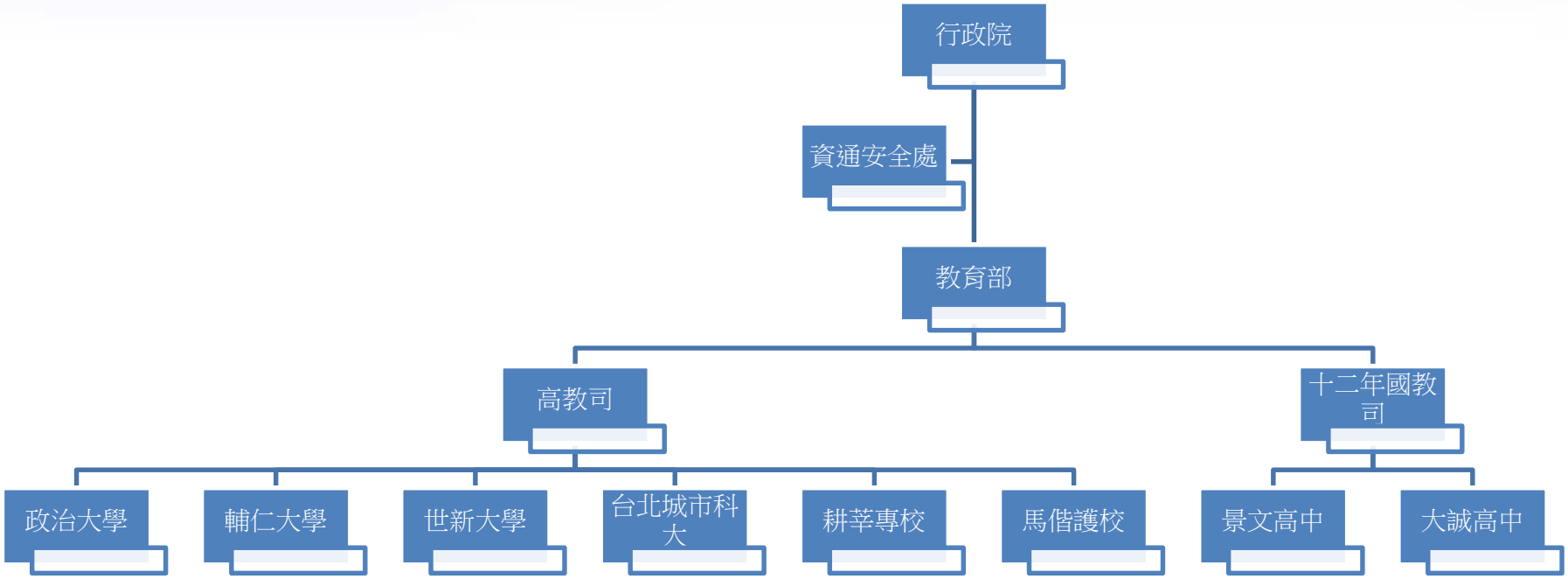
3月下旬
- 修正內部人員獎懲辦法

1月下旬
- 提報自身及所屬機關資安維護計畫實施情形



連線單位面對資安法之應因建議淺見

組織架構


行政院
資通安全處
教育部
高教司
十二年國教司
政治大學
輔仁大學
世新大學
台北城市科大
耕莘專校
馬偕護校
景文高中
大誠高中

A級機關(構)及學校

- 本部各級機關(構)、所管各財團法人及學校符合行政院「資通安全責任等級分級辦法」第四條規定單位。
- 全國性民眾或公務員個人資料檔案之持有或處理、全國性跨公務機關共用性資通系統之維運。
- 辦理大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構或代管常設試務機構 。
- 機關(構)或學校之機房，設有辦理大學、技專校院及高級中等學校等入學考試、甄選、招生等常設試務機構核心系統。
- 承接具國家安全機密性或敏感性業務或技術研究之學院或系所，其研究領域如下：
  - 涉及國家安全資訊、國家機密資訊之領域
  - 涉及國家安全技術、國家機密技術領域

B級機關(構)及學校

- 本部各級機關(構)、所管各財團法人及學校符合行政院「資通安全責任等級分級辦法」第五條規定單位。
- 辦理專科學校、十二年國教入學考試、甄選、招生工作等輪流辦理之試務機構與學校；各項評鑑工作之評鑑機構。
- 臺灣學術網路各區域網路中心。
- 各直轄市及縣(市)教育網路中心。
- 各公私立大學 (區域性或地區性民眾個人資料檔案之持有或處理)。
- 各公立專科學校

C、D級機關(構)及學校

- C級機關(構)及學校
  - 各私立專科學校
  - 各公立高中(職)以下學校具自行或委外開發核心資通系統，校內並設置該核心資通系統伺服器者。

- D級機關(構)及學校
  - 各公立高中(職)以下學校未有自行或委外開發核心資通系統，或核心資通系統未設置於該校。
  - 各私立高中(職)以下學校

資通安全管理法全面施行，應導入施行資安法之範疇？

- 依資安法規定，全機構之核心資訊系統皆須納入ISMS管轄範圍
- ISMS：資訊安全管理系統 Information Security Management System

- 全機關
- 核心資訊系統
  - 已導入ISMS相關制度者依盤點結果列為核心系統
  - 非導入ISMS相關制度者依「資通系統防護需求分級原則」
    - 機密性、完整性、可用性、法律遵循性
    - 質化判斷
  - 依設立宗旨、組織法規規定之
  - 含校內大部份學生或公務員資料

資通系統防護需求分級原則
資訊系統分類分級辦法

表單編號：

安全等級評估表

功能說明：

業務屬性：□行政類 □業務類　　日期：　年　月　日

影響構面				資訊類別安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
		資訊系統安全等級：		

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估		
	異動		
2. 完整性	初估		
	異動		
3. 可用性	初估		
	異動		
4. 法律遵循性	初估		
	異動		

步驟❷：識別業務屬性

項目		業務屬性
識別業務屬性	初估	
	異動	
備註		

簽核欄

業管單位	承辦人	代理人			
維運單位	系統負責人		代理人		

註：請各機關依本身實際陳核流程調整簽核欄位，原則上，建議簽辦人員包含業務承辦人、業務單位主管、資安人員、資訊主管等。

安全等級

- 普
- 中
- 高

資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	資訊系統安全等級	業務承辦單位	業務承辦人	系統負責人	備註
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							

簽核欄	承辦人	直屬主管	單位主管	電算中心主任	資訊安全長

註：請各機關依本身實際陳核流程調整簽核欄位，如：複核主管調整為主任秘書等

- 等級為**高**者
- 依**設立宗旨**、**組織法規**規定之
- **含校內大部份學生或公務員資料**

A級機關(構)及學校

管理面

- 資通系統分級及防護基準
- 資訊安全管理系統之導入及通過公正第三方之驗證
- 配置資通安全專責人員四名
- 人員應持有資通安全專業證照總計四張
- 每年辦理二次內部資通安全稽核
- 每年辦理一次核心資通系統業務持續運作演練

技術面

- 安全性檢測
  - 系統弱點檢測
  - 系統滲透測試
- 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
  - 防毒軟體
  - 網路防火牆
  - APT及郵件過濾機制
  - 入侵偵測及防禦機制
  - 對外服務之核心系統應用程式防火牆
  - 進階持續性威脅攻擊防禦措施 (部內已建置)
- 資通安全教育訓練

B級機關(構)及學校 應辦事項

管理面

- 資通系統分級及防護基準
- 資訊安全管理系統之導入及通過公正第三方之驗證
- 配置資通安全專責人員二名
- 人員應持有資通安全證照總計二張　、資安評量證書二張。
- 每年辦理一次內部資通安全稽核
- 每年辦理一次核心資通系統業務持續運作演練
- 每年辦理一次資安治理成熟度評估
- 全部核心資通系統，每兩年辦理１次業務持續運作演練

技術面

- 安全性檢測
  - 核心系統弱點檢測　每１年一次
  - 核心系統滲透測試　每２年一次
- 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
  - 防毒軟體
  - 網路防火牆
  - 郵件過濾機制
  - 入侵偵測及防禦機制
  - 對外服務之核心系統應用程式防火牆
- 資通安全教育訓練

C級機關(構)及學校

管理面

- 資通系統分級及防護基準
- 資訊安全管理系統之導入及通過公正第三方之驗證
- 配置資通安全專責人員一名
- 人員應持有資通安全證照總計一張、資安評量證書一張。
- 每二年辦理一次內部資通安全稽核
- 每二年辦理一次核心資通系統業務持續運作演練

技術面

- 安全性檢測
  - 核心系統弱點檢測
  - 核心系統滲透測試
- 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
  - 防毒軟體
  - 網路防火牆
  - APT及郵件過濾機制
- 資通安全教育訓練

D級機關(構)及學校

- 資通安全防護
  - 防毒軟體
  - 網路防火牆
  - APT及郵件過濾機制
- 資通安全教育訓練
  - 每人每年三小時教通安全教育訓練

緩衝期

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	

時程簡述

108

確認範圍

- 盤點、確認驗證系統
- 確認應執行項目

向上級單位提案

- 校內相關處室協助
- 教育訓練
- 費用支援

1. 自行執行或尋求外部顧問機構
2. 費用估計

109年

照案執行

教育訓練、推廣

抽檢

110年

驗證

- 教育體系資通安全驗證

例外，但很重要的...GCB

- 因為本區網沒有ＡＤ，所以例外了.....
- 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。
- 對象
  - 使用AD驗證者
- 說明文件：行政院國家資通安全會報技術服務中心

- 驗證時程：**108年年底**前須完成。

感謝聆聽！