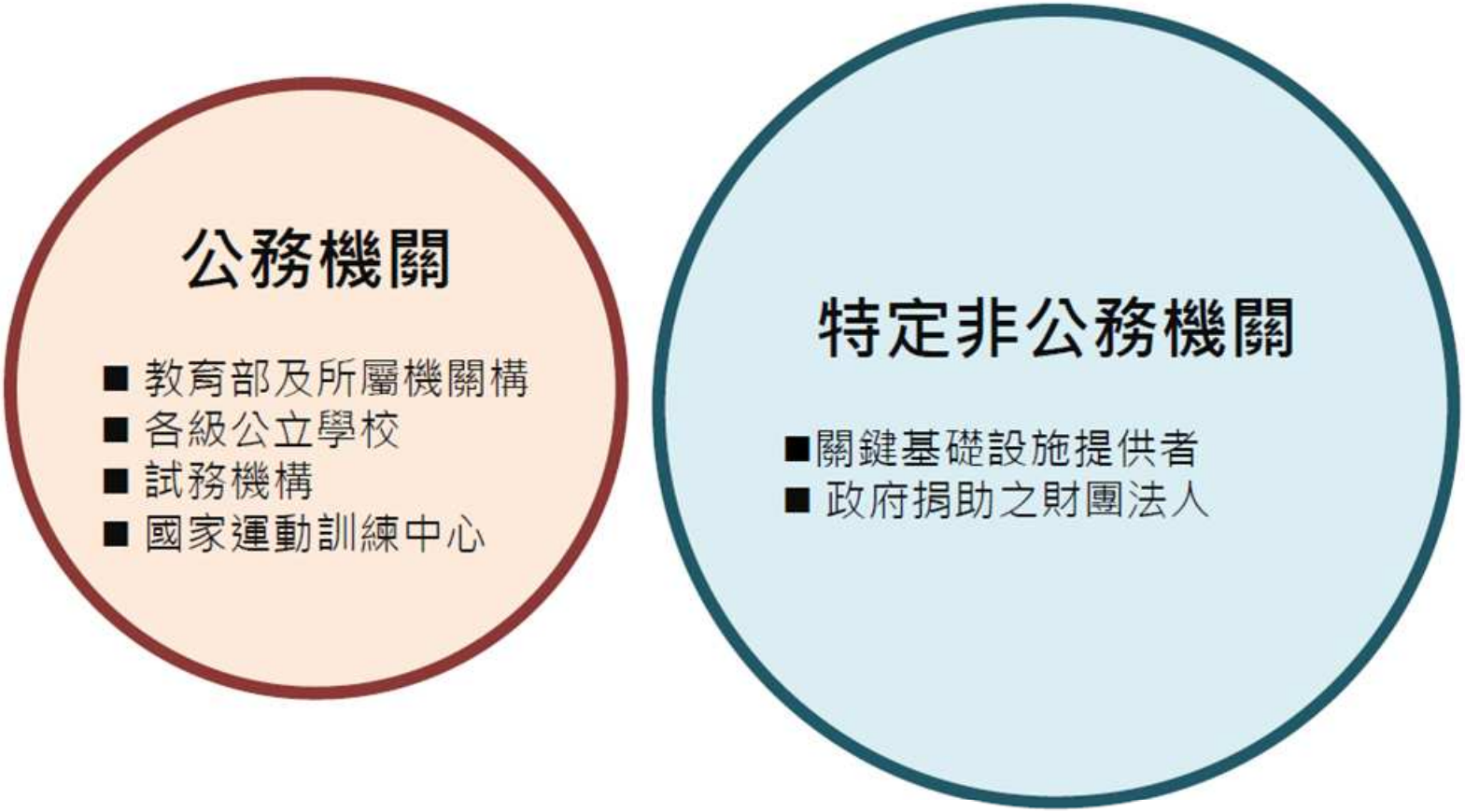
資通安全管理法教育體系之法遵說明

桃園區域網路中心
(國立中央大學電子計算機中心)
技正張二川

資通安全管理法

- 總統107年6月6日公布資通安全管理法。
- 行政院107年11月21日發布相關子法：
  - 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
- 行政院107年12月05日函定自108年1月1日施行。

教育體系規範對象


公務機關
■ 教育部及所屬機關構
■ 各級公立學校
■ 試務機構
■ 國家運動訓練中心
特定非公務機關
■關鍵基礎設施提供者
■ 政府捐助之財團法人

教育體系資安責任等級分級原則

	A級	B級	C級	D級
業務個資	■教育部 ■承接敏感業務、研究學校	■公立大專校院		
資通系統		■國家教育研究院 ■國家圖書館	■部屬機構（電台、博物館、圖書館） ■國家運動訓練中心 ■公立高級中等以下學校（有核心資通系統）	■公立高級中等以下學校（已向上集中無維運核心資通系統，無機房或僅設置通訊機房）
機關層級	■大學附設醫院（醫學中心）	■大學附設醫院（區域、地區醫院）		

*核心資通系統指依「資通安全管理法施行細則」第7條第2項：

- 支持各校「核心業務」持續運作必要之系統。
- 依分級辦法附表九「資通系統防護需求分級原則」，資通系統判定其防護需求等級為高者。

核心資通系統

- 支持各校核心業務持續運作之必要系統。
  - 如教務相關系統，或持有教師、學生重要個資系統。

- 依分級辦法附表分級原則，系統等級為高者。
  - 機敏性、完整性、可用性、法律遵循性。

資通安全責任等級
-教育體系等級提交機關

- 提交機關應每2年提交所屬責任等級，報行政院核定。
  - 教育部（行政院直屬機關）
    - 部屬機關、機構
    - 國立大專校院
    - 國立高級中等以下學校(由國教署負責)
    - 教育部主管政府捐助之財團法人
  - 各直轄市、縣（市）政府
    - 縣（市）立各級學校

分級作業辦法應辦事項

分級作業辦法應辦事項-管理面

辦理事項	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		2年內
ISMS之導入及通過公正第三方之驗證	2年內全部核心資通系統導入資訊安全管理系統。	3年內完成第三方驗證；並持續維持期驗證有效性。		O*
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	
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專職(責)人員（1年內）		4人	2人	1人*
資安治理成熟度評估（公務機關）		每年1次		X

***C級單位因應措施**

- ISMS導入
  - 短期：資科司後續將與國教署協調規劃**輔導團隊**，輔導C級學校導入教版管理規範。
  - 長期：高級中等以下學校全部**核心系統向上集中**為共通系統，將責任等級降至D級。
- 專職(責)人員
  - 短期：本部同意高級中等以下學校得以專責人員配置，兼任資訊行政教師減授教學節數。
  - 長期：國教署配合修正「高級中等學校組織設置及員額編制標準」，資安人力法制化。

分級作業辦法應辦事項-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
	系統滲透測試	每年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設定檢視	每年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		X
	依行政院指定方式提交監控管理資料	O	O	X
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		
	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		X
	APT攻擊防禦	1年內	X	
政府組態基準 （GCB）	依主管機關公告之項目，完成GCB導入作業，並持續維運（公務機關）	1年內		X

應辦事項配套措施-技術面

應辦單位	辦理項目	因應措施
A、B、C級	網站安全弱點檢測	由**成功大學網站防護團隊**協助辦理。
	ABC級系統滲透測試	資科司將規劃**教育體系技術團隊**協助辦理。
	資通安全健診	請**北、南區學術資訊安全維運中心**協助辦理相關教育訓練課程。
A、B級	資通安全威脅偵測管理機制	**臺灣學術網路連線單位**可結合**臺灣學術網路資安監控系統（南、北SOC, Mini-SOC）**進行威脅偵測機制。

分級作業辦法應辦事項-認知與訓練

辦理事項	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每人每年各接受12小時之資通安全專業課程訓練或資通安全職能訓練*	至少4人	至少2人	至少1人
	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	每人3小時		
資通安全專業證照及職能訓練證書	初次受核定或等及變更後之一年內，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張以上	2張以上	1張以上
	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張以上	2張以上	1張以上

分級作業辦法應辦事項-D、E級

面向	辦理項目	辦理細項	D	E
技術面	資通安全防護	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	X
認知與訓練	資通安全教育訓練	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	每人3小時	

教育體系因應資通安全管理法之規劃說明-教育部資訊及科技教育司

教育體系資安責任等級因應措施

- 教育體系各單位任務編組（區域網路中心、縣市教育網路中心）視同內部單位，不另提責任等級、資通安全維護計畫。

- 因公私立學校應有一致性規範，後續私立學校，資科司依「資通安全分級作業辦法」修訂「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」一併規範。

訂定資通安全維護計畫

- 本法第10條，公務機關應訂定及實施資通安全維護計畫。
- 本法第12條，公務機關應每年向上級提出資通安全維護計畫實施情形。
- 本法第13條，公務機關應稽核其所屬機關之資通安全維護計畫實施情形。

109年資通安全稽核-作業階段及時程

階段	作業時程	重點工作
一	準備作業(2-3月)	研擬稽核計畫、受稽機關、稽核委員建議名單及稽核項目等
二	前置作業(4月)	1.確認稽核計畫 2.確認受稽機關與時程 3.確認稽核委員與觀察員名單
三	實施作業 (5-12月)	進行實地稽核
四	檢討作業 (12月-110年1月)	提出稽核結果及共同與個別發現事項、建議 表揚優良機關、研擬立法院之稽核概況報告

1個月前發文受稽機關

對象	稽核 期間	通知日期及方式	協調 稽核日期
受稽機關	第2季5-6月	稽核前1個月 函文通知	發文前
	第3季7-9月		
	第4季10-12月		

稽核計畫 - 稽核準則

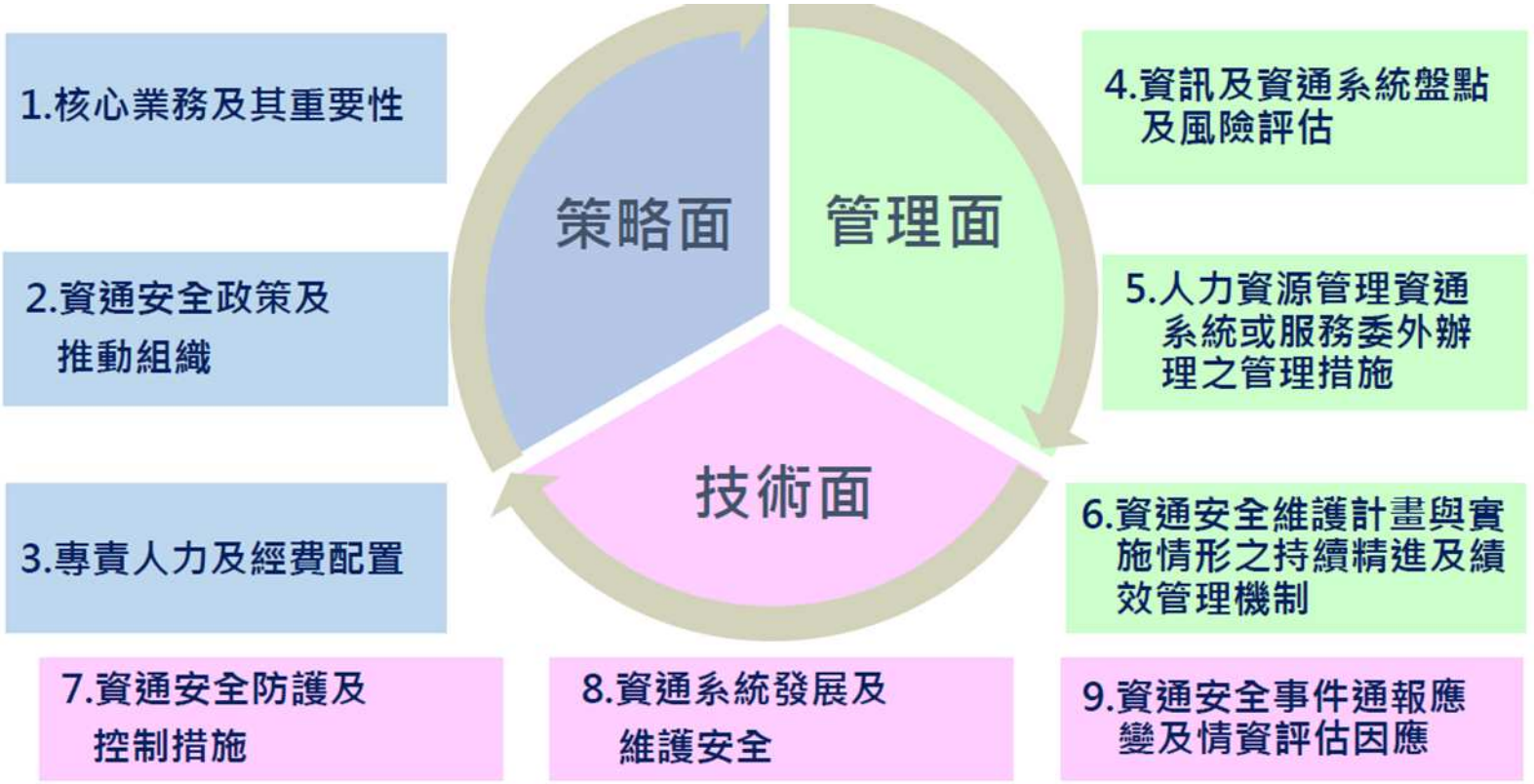
- 資通安全管理法及其子法
- 受稽機關之資通安全維護計畫
- 資訊安全管理系統國家標準 CNS 27001:2014國際資訊安全管理標準 ISO 27001:2013)
- 國際資訊服務管理標準 ISO 20000:2018

稽核計畫 - 稽核範圍及方式

- 稽核範圍
  - 受稽機關資通安全維護計畫所包括之全機關及核心資通系統之各項資通安全管理政策、程序等

- 稽核方式
  - 一般稽核(實地稽核)
  - 第二方-稽核輔導

作業方式 - 實地稽核項目



- 實地稽核項目檢核表，依「資通安全管理法」相關規定之不同，分為公務機關、特定非公務機關2式

項次	稽核項目	稽核重點說明
1	核心業務及其重要性	• 確認資通系統分級 • 確認資訊安全管理系統(ISMS)之範圍 • 確認機關業務持續之營運衝擊分析 • 確認核心資通系統持續運作計畫 • 確認業務持續運作演練 • 確認備份及備援機制 • 確認復原測試 • 資安治理成熟度評估
2	資通安全政策及推動組織	• 確認資安政策及目標 • 確認受稽機關之資安管理及運作 • 確認資安組織推動 • 確認績效評估、考核機制 • 確認利害關係人管理等
3	專責人力及經費配置	• 確認資安經費及資安人力等資源配置之妥適性 • 確認資安/資訊經費占經費比率 • 確認資安人力配置情形等 • 確認人員資安作業程序 • 確認資安認知及訓練 • 確認機關人員對於資安防護工作之落實

項次	稽核項目	稽核重點說明
4	資訊及資通系統盤點及風險評估	• 確認資訊資產盤點及相關管理程序 • 確認資訊資產處置規範與異動汰除管控作業 • 確認風險評估、風險處理及後續追蹤情形
5	資通系統或服務委外辦理之管理措施	• 確認資訊作業委外安全管理程序 • 確認資訊委外資安要求及服務等級協議 • 確認委外人員管理 • 確認委外供應商之管理、監督及稽核
6	資通安全維護計畫與實施情形之持續精進及績效管理機制	• 確認機關資通安全計畫訂定、修正及實施情形 • 確認內部稽核及後續追蹤 • 確認上級/監督/中央目的事業主管機關之監督管理辦理情形 • 確認對於所屬/所監督/所管之機關稽核作業 • 確認對於所屬/所監督/所管之機關資安事件之審核 • 確認對於所屬/所監督/所管之機關資通安全演練之實施

項次	稽核項目	稽核重點說明
7	資通安全防護及控制措施	• 確認安全性檢測實施情形 • 確認資通安全健診、資通安全防護實施情形 • 確認資通系統及相關設備監控 • 確認使用紀錄管理 • 確認政府組態基準實施情形 • 確認電子資料安全管理機制 • 確認網路規劃及管理 • 確認資料處理、儲存及傳輸安全 • 確認電子資料相關設備管理 • 確認行動裝置安全、軟體使用安全、網路即時通訊安全及電子郵件安全
8	資通系統發展及維護安全	• 確認資通系統之防護需求 • 確認SSDLC各個階段之安全檢核，包括系統需求、設計、開發、測試、驗收時應注意之安全措施 • 確認資通系統之變更管制程序
9	資通安全事件通報應變及情資評估因應	• 確認情資分享機制 • 確認資安事件通報及應變作業規範及落實 • 確認資安事件改善措施之有效性

構面	實地稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資訊及資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10
合計		100