深化各機關落實資訊安全管理系統CNS27001規劃

行政院資通安全處

108年12月

大綱

- 前言
- 資訊作業委外管理現況
- 資訊安全管理系統目的及效益
- 政府機關推動現況
- 常見問題及精進作為
- 結論與建議

前言

- 延續上個報告之資安事件
  - OO部資通系統遭駭
  - 某醫院內部人員帳號遭駭客盜用
  - 某醫療院所資訊服務廠商遭駭客入侵

- 根因分析
  - 資訊資產存取權限控管機制待加強
  - 安全性檢測及管理驗證機制未有效發揮
  - 資訊作業委外安全管理未落實

大綱

- 前言
- 資訊作業委外管理現況
- 資訊安全管理系統目的及效益
- 政府機關推動現況
- 常見問題及精進作為
- 結論與建議

資訊作業委外管理現況

規劃 → 開發 → 維運

資通系統

資通安全管理法第9條、資通安全管理法施行細則第4條、
資通安全責任等級應辦事項、資通系統防護基準
資通安全維護計畫-第12章資通系統或服務委外辦理之管理
採購法及資訊服務採購契約範本
政府資訊作業委外安全參考指引、安全系統發展生命週期SSDLC

輔導 → 驗證

管理制度

資通安全管理法施行細則第4條
資通安全責任等級應辦事項
資訊安全管理系統（ISMS）RFP
資訊安全管理系統（ISMS）第三方驗證RFP
CNS 27001 / ISO 27001

大綱

- 前言
- 資訊作業委外管理現況
- 資訊安全管理系統目的及效益
- 政府機關推動現況
- 常見問題及精進作為
- 結論與建議

導入資訊安全管理系統目的

- **規劃面**：使資安風險得以系統化進行分析及管理
- **執行面**：使資訊資產具備機密性、完整性及可用性
- **查核面**：使機關瞭解自身資安弱點及風險缺失
- **精進面**：使機關強化風險管理並擁有可信賴之資通訊環境

導入資訊安全管理系統效益分析

比較項目	導入前	導入後
設定安全目標	未明確設定	可衡量指標
了解風險來源	被動回應	積極回應
業務承擔風險	風險高	風險降至可接受之等級
使用者操作信心	信心不足	信心高
使用者資安滿意度	滿意度低	滿意度高
資訊安全管理難度	分散式的資安管理	系統的資安管理
資安事件回應速度	事件處理人力 未有效管理	建立事件回應機制
資訊作業效率	人員經驗分享 效率低	定義SOP，效率高
內部稽核能力	缺乏專業人力	具規劃與實務能力

大綱

- 前言
- 資訊作業委外管理現況
- 資訊安全管理系統目的及效益
- 政府機關推動現況
- 常見問題及精進作為
- 結論與建議

政府機關推動歷程

- **第一期(90-93年)**：推動實施資訊安全管理制度
  - 針對20多個影響國家安全、社會安定的重要資訊作業系統，要求限期通過國際資訊安全管理系統驗證
- **第二期(94-97年)**：推動資訊安全管理系統驗證
  - 政府機關依部門、系統、業務及實體區域等，要求資安等級A、B級機關應分於96、97年認證通過驗證
- **第四期(102-105年)**：修改分級作業規定
  - 資安等級A、B級機關應分別於105、106年前完成導入，並於隔年通過第三方驗證
- **資通安全管理法**：
  - 於108年1月1日正式實施

法遵要求

責任等級	應辦事項
A級機關 B級機關	初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，**於三年內完成公正第三方驗證，並持續維持其驗證有效性**
C級機關	初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入

「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構

我國ISMS輔導及驗證現況(1/2)

- 2017年政府機關、學校、企業抽樣調查結果

項目	整體		政府機關		學校		企業	
	N=5,283		N=1,578		N=2,535		N=1,170	
ISMS輔導	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)
	1,241	23.5%	407	25.8%	721	28.4%	113	9.7%
第三方驗證	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)
	598	48.2%	264	64.9%	277	38.4%	57	50.4%

資料來源：國家資通安全會報技術服務中心106年資安現況調查報告

我國ISMS輔導及驗證現況(2/2)

- 2017年政府機關抽樣調查結果（依機關責任等級分析）

項目	整體		A級		B級		C級		D級	
	N=1,578		N=66		N=280		N=712		N=520	
ISMS輔導	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)	個數(N1)	%=(N1/N)
	407	25.8%	N1=63	95.5%	171	61.1%	112	15.7%	61	11.7%
第三方驗證	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)	個數(N2)	%=(N2/N1)
	264	64.9%	N2=61	96.8%	123	71.9%	59	52.7%	21	34.4%

資料來源：國家資通安全會報技術服務中心106年資安現況調查報告

大綱

- 前言
- 資訊作業委外管理現況
- 資訊安全管理系統目的及效益
- 政府機關推動現況
- 常見問題及精進作為
- 結論與建議

資訊安全管理系統導入常見問題

- 資安推動組織參與之業務單位涵蓋面及參與度不足
- 欠缺完整的個人資料管理制度
- 資訊系統分級未確實進行衝擊影響評估，部分資訊系統之安全等級被低估
- 缺乏對委外廠商之資安要求及有效監督與管理

精進作為

- 資安推動組織宜由資通安全長召集各單位之主管或副主管組成
- 個人資料以作業流程面向進行盤點，並訂定管理規範及設立推動組織
- 詳實盤點資訊系統，並遵循資通安全責任等級分級辦法規定
- 對委外廠商詳訂作業程序與規範，並強化機關監督管理權責

資訊安全管理系統驗證常見問題

- 驗證流於形式
- 未擴及業務單位
- 未涵蓋核心業務持續運作之必要系統
- 稽核深度不足
- 驗證服務獨立性不夠

精進作為

資通安全處

- 推動ISMS驗證服務上架至共同供應契約平台
- 強化根因分析作為，必要時公布相關內容

各機關

- 擴大驗證範圍
- 輔導與驗證服務契約，獨立招標
- 落實委外廠商稽核作業

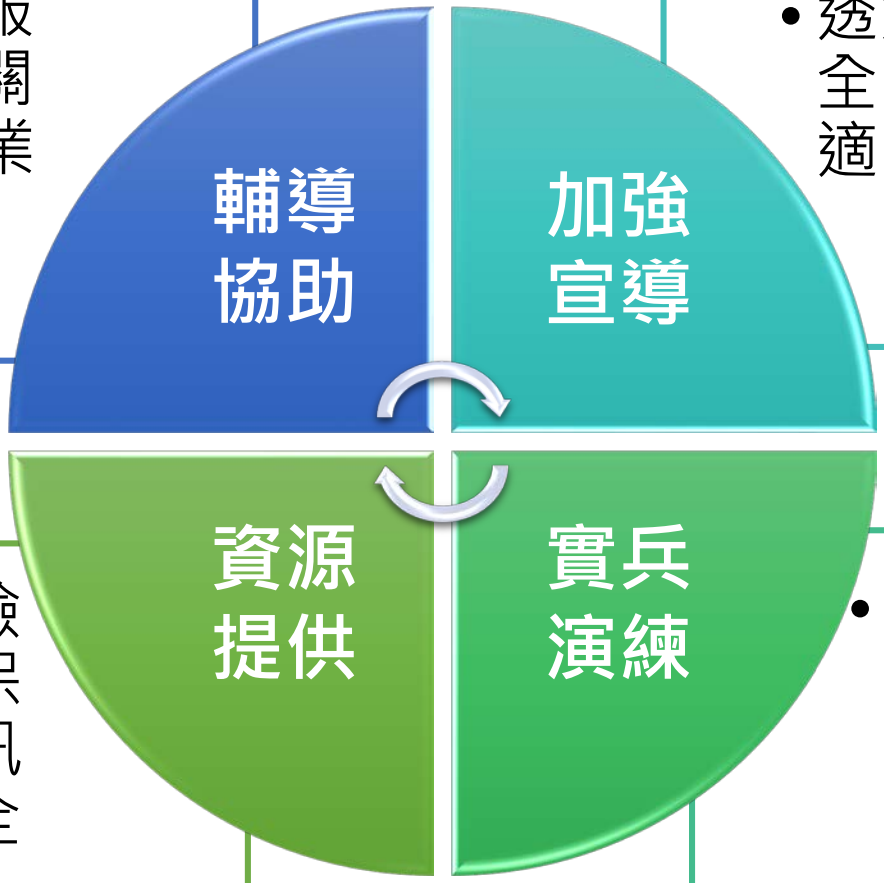
大綱

- 前言
- 資訊作業委外管理現況
- 資訊安全管理系統目的及效益
- 政府機關推動現況
- 常見問題及精進作為
- 結論與建議

結論與建議

- 每年由資安服務團輔導機關落實委外作業安全管理

- 透過資安長會議或全國巡迴說明會等適當場合加強宣導



- 資通系統風險評鑑、個資保護、政府資訊作業委外安全等參考指引

- 透過相關資通安全演練驗證機關資安作業落實度

謝謝聆聽
敬請指教