政府資訊服務採購暨資安入規整體推動作法、契約範本與指引說明

行政院公共工程委員會

112年8月11日

大　綱

壹、現況說明

貳、解決策略

參、工作歷程

肆、具體作法

伍、結語

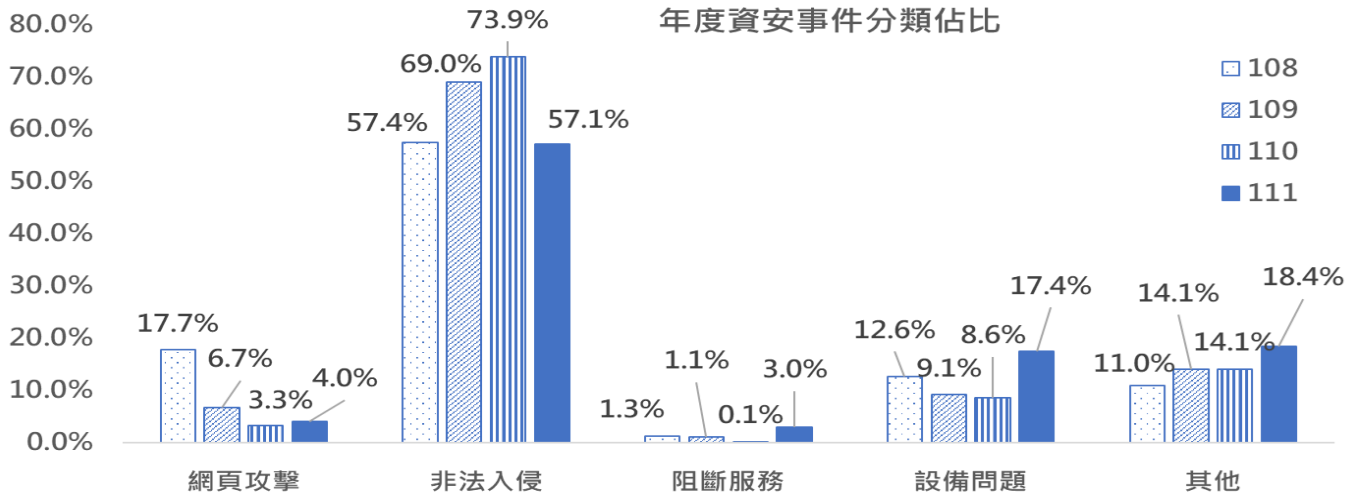
壹、現況說明

電子化政府須有安全與完善的資訊架構

壹、現況說明

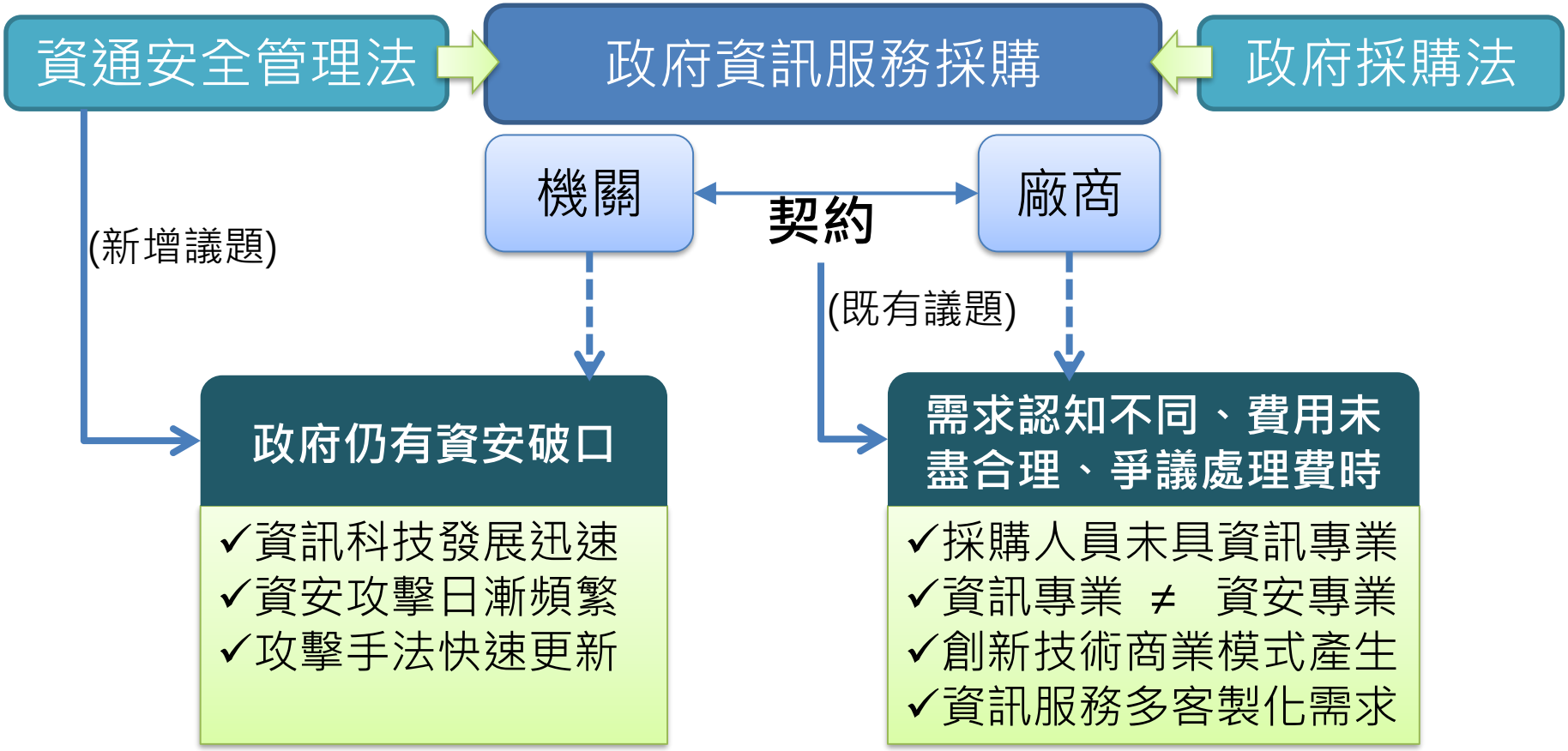
資訊、資安快速變遷；TikTok、ChatGPT分別在9、2個月內達到1億使用者；**資安攻擊手法3-6個月翻新一個世代**。

我國近年公務機關通報資安事件統計表				
年度	事件數	1級事件	2級事件	3級事件
109	525	451	65	9
110	696	619	66	11
111	597	493	94	10
合計	1818	1563	225	30

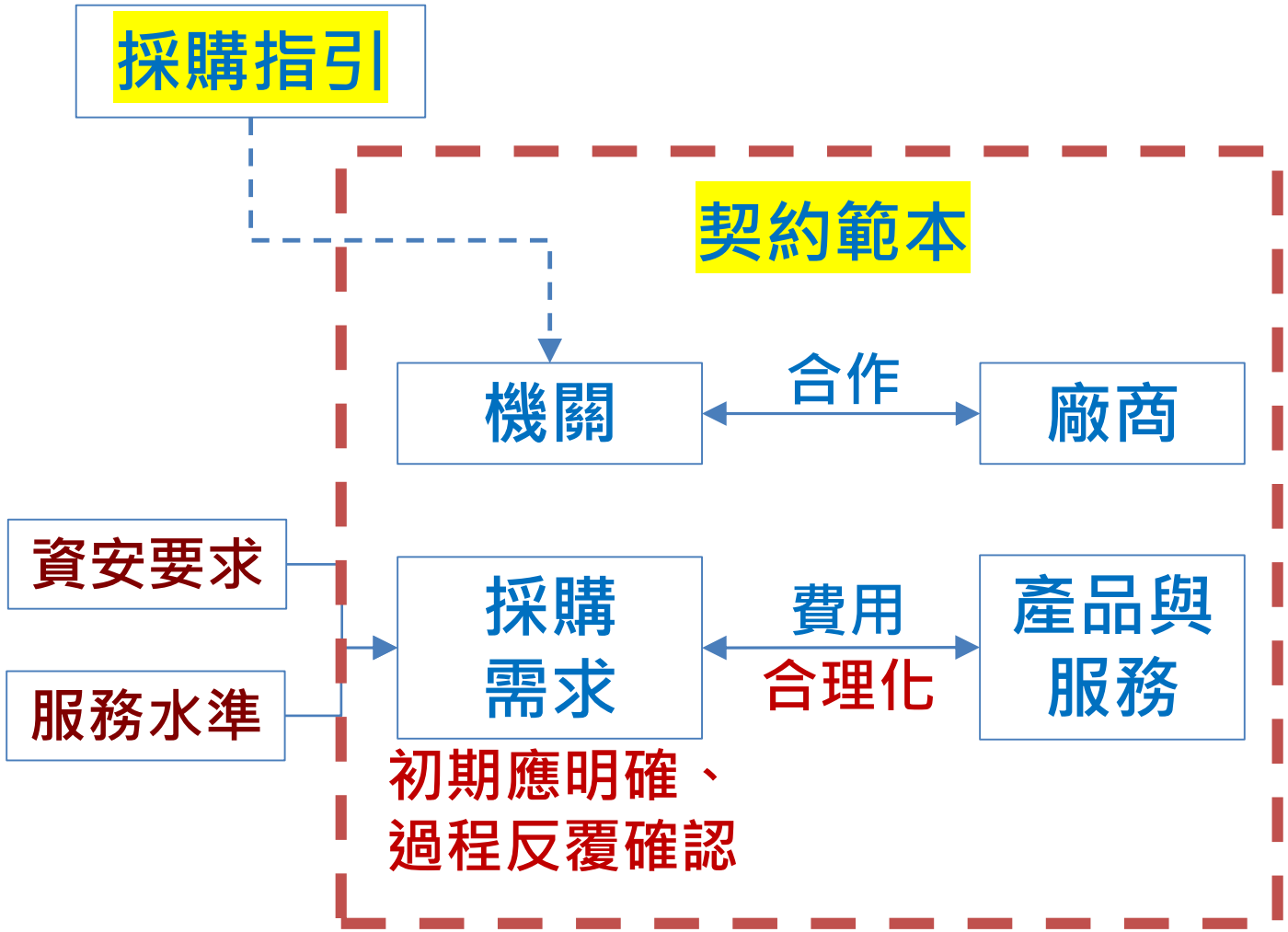


壹、現況說明

機關資訊服務採購現況

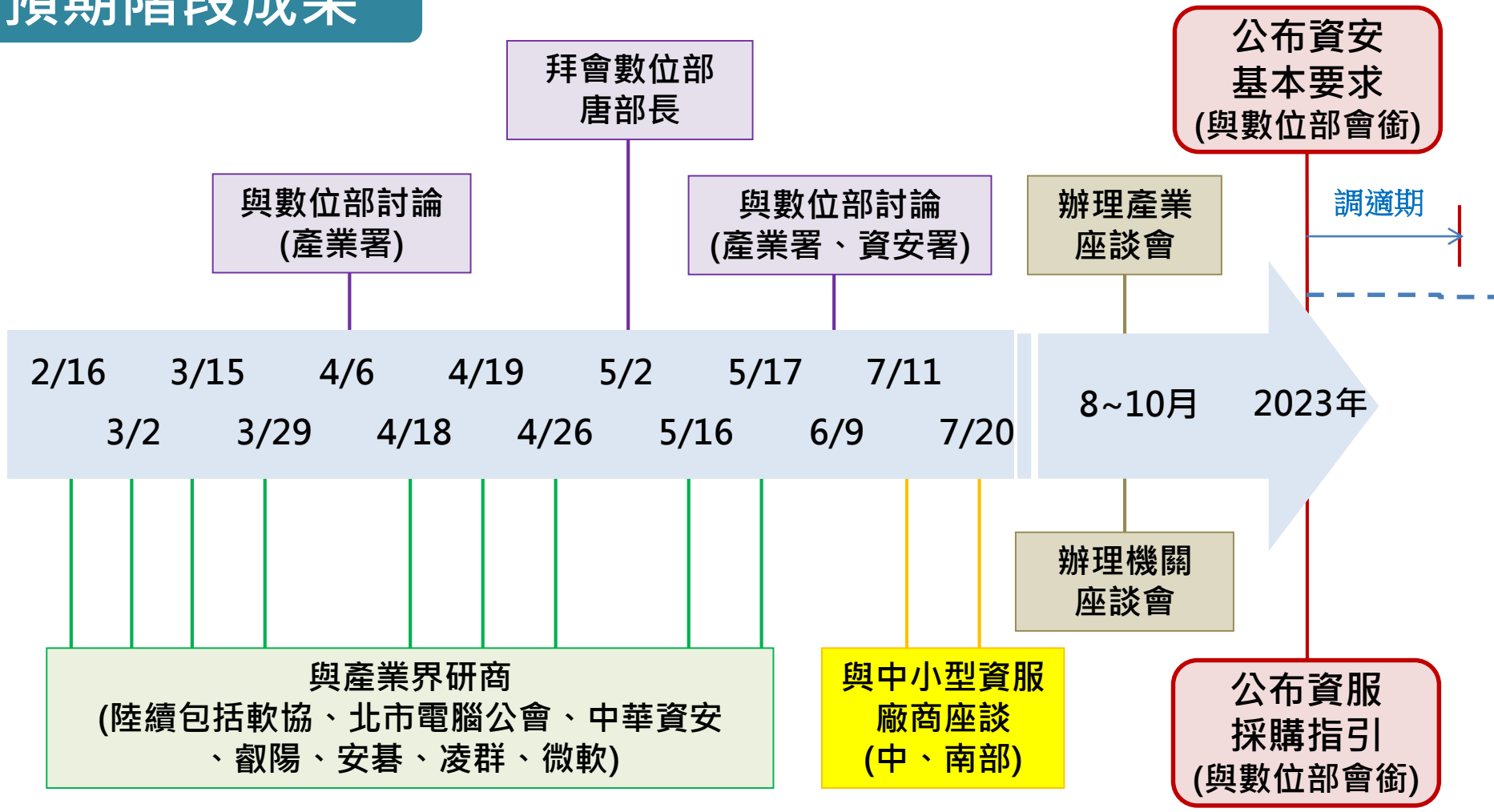


貳、解決策略



參、工作歷程

預期階段成果



肆、具體作法-落實資安、載明服務水準

契約範本增列-資安基本要求及服務水準

- 參考汽車DM，規格區分標配、選配，符合機關個案採購需求

系統資安分級		資服類型		契約需求
• 高-機敏 • 中-關鍵資訊基礎設施(CII) • 普-一般 *配合資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)。	+	• 雲端微服務(SaaS) ①套裝型 ②辦公室生產力工具 ③客製化需求更版 • 雲端平台(PaaS/IaaS) • 資服規劃 • 資安規劃 • 系統開發 • 功能擴充 • 系統維護	→	• 資安分級要求 • 系統服務水準(SLA)

肆、具體作法-資服契約範本資安基本要求

雲端微服務(SaaS)	• 通過ISO認證、身分鑑別、資料傳輸機密完整、日誌保存、安全要求等
雲端平台(PaaS/IaaS)	• 同SaaS。另增加營運計畫、變更管理、資安監控、資安演練、第三方檢測等
資服規劃標案	• 符合機關資安政策
資安規劃標案	• 審視機關資安規劃
系統開發	• 同PaaS。另增加應用程式安全、存取控制、與其他系統介接、資安人員及教育訓練、資安成熟度等
既有功能擴充	• 國際規範、SSDLC或同級認證、程式碼安全、第三方檢測、教育訓練等
系統維護營運	• 符合機關資安政策

肆、具體作法-資服契約範本資安基本要求

雲端微服務-SaaS套裝型 (以系統資安分級「高」為例)

- 提供服務商：須符合國際標準(如：ISO27001)、非陸資
- 事件日誌保存與可歸責性
- 供應商安全要求：廠商提供安全要求佐證資料，由機關資安長確認

肆、具體作法-資服契約範本資安基本要求

雲端微服務-SaaS辦公室生產力工具

(以系統資安分級「高」為例)

- 基本同SaaS套裝型。
- 防惡意軟體、連結：靜態、動態沙箱分析
- 防釣魚郵件：郵件過濾及身分辨識
- 資料與個資安全：加密、外洩防護等
- 身分驗證與存取控制：多因子認證、零信任措施

既有雲端微服務-SaaS客製化更版

(以系統資安分級「高」為例)

- 供應商安全要求：廠商提供安全要求佐證資料，由機關資安長確認

肆、具體作法-資服契約範本資安基本要求

雲端平台-PaaS/IaaS

(以系統資安分級「高」為例)

- 提供平台服務商：須符合國際標準(如：ISO27001)、非陸資、第三方檢測廠商等級
- 弱點管理：平台服務漏洞定期檢視
- 存取控制：帳號、資料傳輸管控、多因子鑑別。
- 變更/安全管理：應有相關管理制度
- 資料安全：相關安全措施
- 資安防護建置持續監控：網路實體入侵防護、監測等
- 資安演練：模擬演練等
- 第三方檢測：弱點掃描、滲透測試等

肆、具體作法-資服契約範本資安基本要求

資服規劃標案

(以系統資安分級「高」為例)

- 提供平台服務商：非陸資
- 標案內容需納入資安政策：符合機關資安規範要求

資安規劃標案

(以系統資安分級「高」為例)

- 提供平台服務商：非陸資
- 協助審視機關資安規劃：協助機關強化資安措施

肆、具體作法-資服契約範本資安基本要求

系統開發 (以系統資安分級「高」為例)

- 提供平台服務商：須符合國際標準(如：ISO27001)、非陸資、第三方檢測廠商等級等
- 符合國際標準規範：導入國際標準及取得驗證
- 應用程式安全
- 存取控制：應有相關管理制度
- 事件日誌保存及可歸責性
- 營運持續計畫
- 身分識別與鑑別

肆、具體作法-資服契約範本資安基本要求

系統開發

(以系統資安分級「高」為例)

- 系統與服務獲得、通訊保護、資訊完整性：依系統防護需求等級，辦理相關措施。
- 與其它平台系統API介接：介接時傳輸加密、稽核紀錄等。
- 資安防護建置持續監控：網路實體入侵防護、監測等
- 資安維運服務、演練、專責人員、教育訓練
- 第三方檢測：弱點掃描、滲透測試等

肆、具體作法-資服契約範本資安基本要求

系統後續擴充 (以系統資安分級「高」為例)

- 提供平台服務商
- 符合國際標準規範
- 程式碼安全：提供SBOM表
- 第三方檢測：弱點掃描、滲透測試等
- 資安教育訓練

肆、具體作法-資服契約範本資安基本要求

軟體或系統維運 (以系統資安分級「高」為例)

- 符合機關資安政策
- 應用程式安全：提供SBOM表
- 第三方檢測：弱點掃描、滲透測試等

肆、具體作法-費用合理編列

資訊服務採購作業指引

階段	重要內容
預算編列	◘ 編列一定比率之資安預算並單獨列項 ◘ 考量檢測費用分擔(履約中查驗、驗收查驗) ◘ 依個案特性編列預備費及物價調整費
招標決標	◘ 載明固定價格決標者不議減價格 (另工程會前於112.5.16工程企字第11200030081函予各機關) ◘ 評選項目不得列「回饋」項目
契約執行	◘ 機關新增需求(包含機關資安等級提升)應合理增加經費及期程價格

肆、具體作法-需求反覆確認

資訊服務採購作業指引

階段	重要內容
預算編列	◘ 必要時先行辦理系統整體規劃 ◘ 依法得洽廠商提供意見
招標決標	◘ 載明服務水準及資安要求等具體需求 ◘ 要求廠商投標時載明執行規劃
契約執行	◘ 反覆確認需求及階段性執行成果 (另工程會前於111.9.22工程資字第1111500157號函檢送「資訊服務採購需求確認之對策與作法」予各機關)

伍、結語

- **資安到位是近年施政的重大挑戰之一，本案秉持*Aim High, Move Fast*精神，翻修資服採購契約範本，並動態更新資安要求。**
- **立即效益**
  - 改善及確保機關資安防護強度
  - 改善採購效率、減少履約爭議
  - 解決資服產業長期反應之訴求
- **長期效益**
  - 以政府採購引導產業資安能力
  - 費用合理，營造產業成長環境

報告完畢