資通安全管理法施行檢討與宣導事項

行政院資通安全處

110年

大綱

一、前言

二、資安維護計畫實施情形

三、資安事件通報

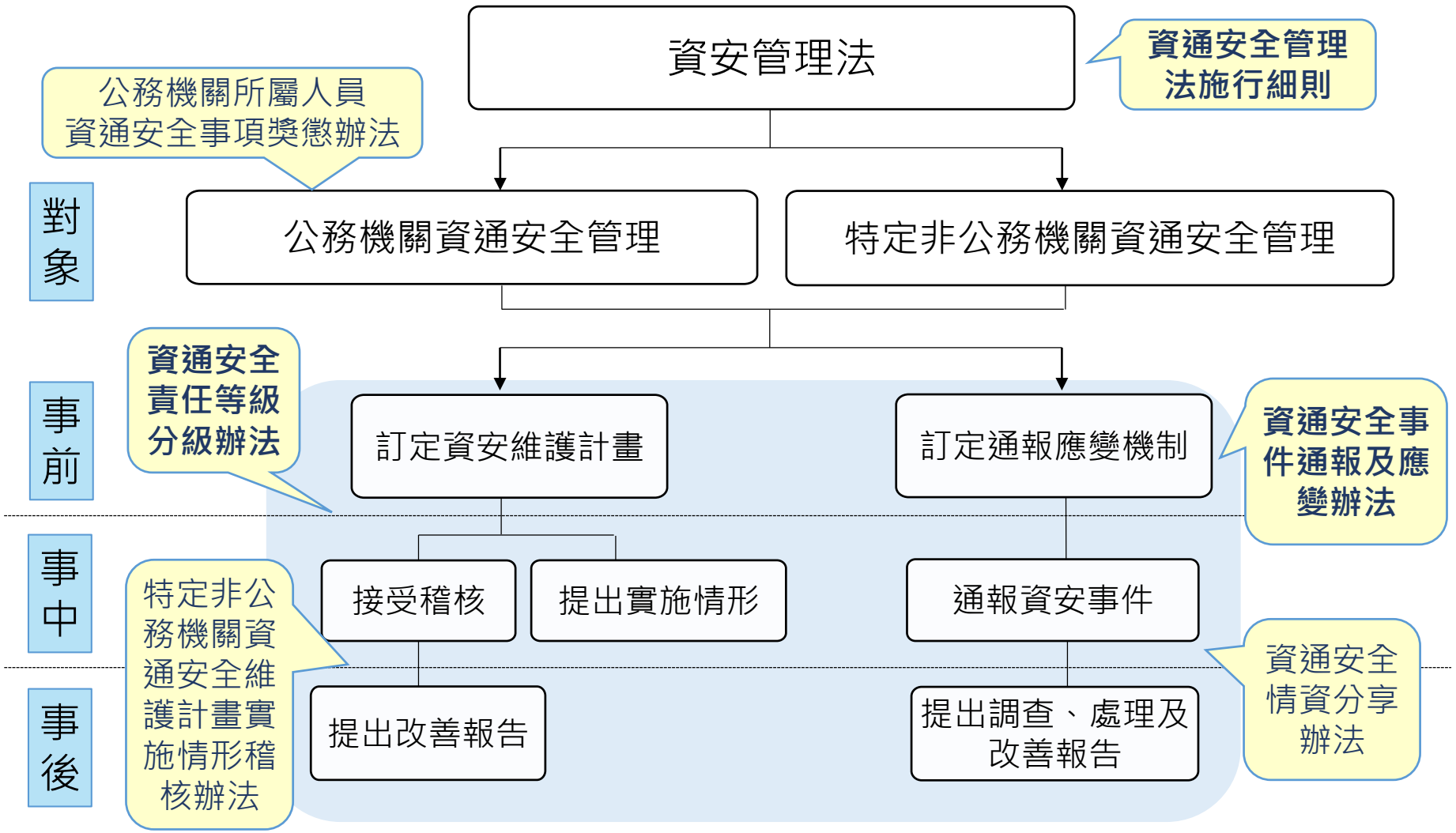
四、資安稽核作業

五、攻防演練

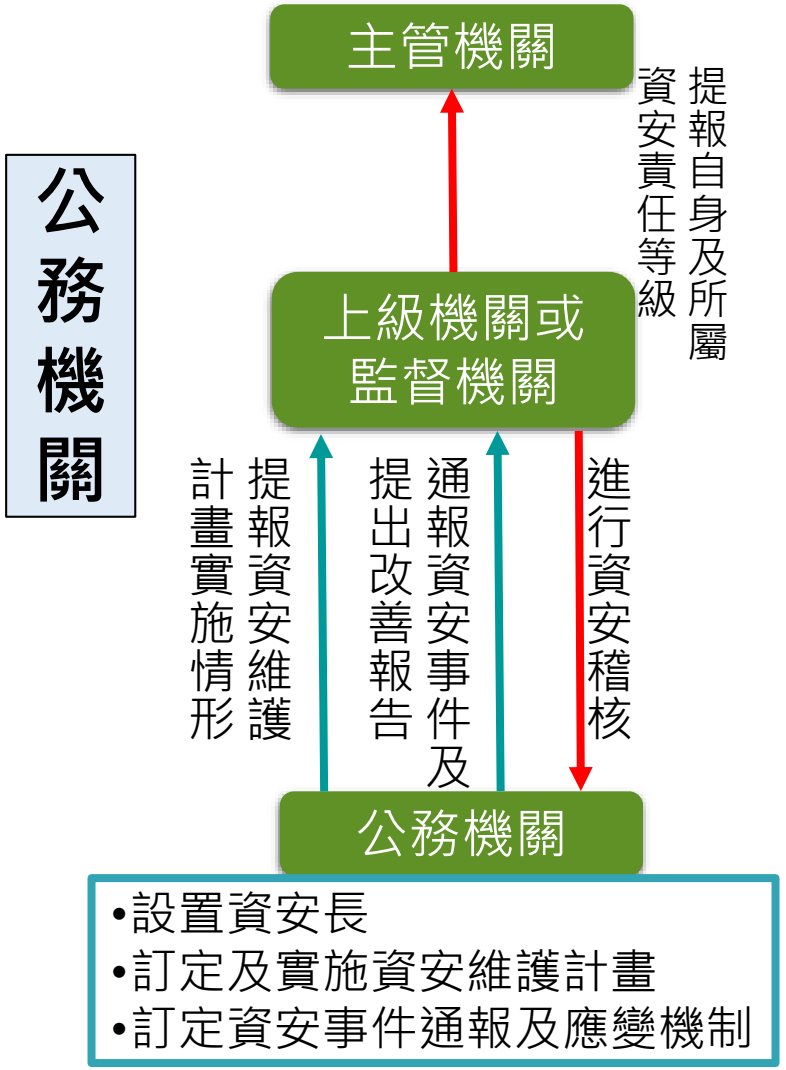
六、近期作業宣導

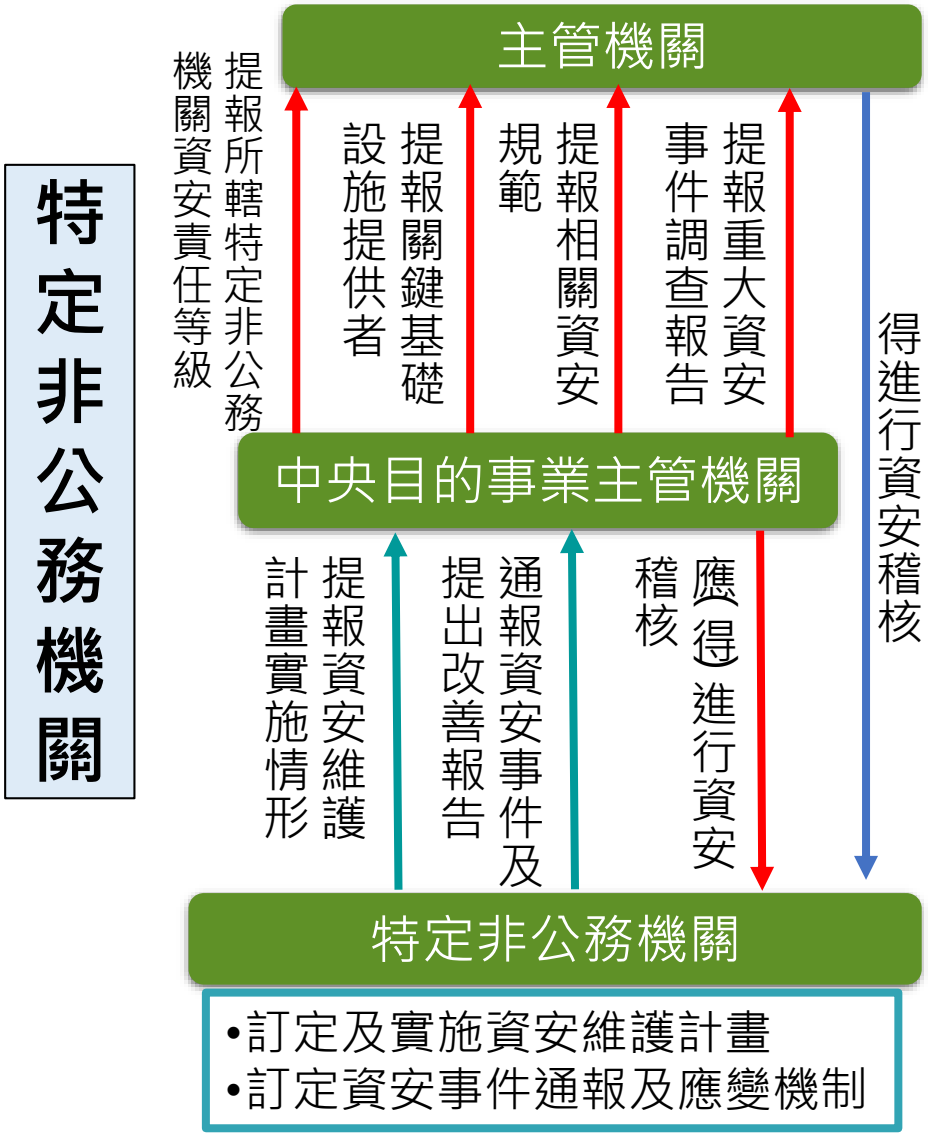
前言

資通安全管理法各子法授權來源



納管機關間之角色與權責





機關資安責任等級核定情形

- 資通安全管理法自108年1月1日開始實施
- 核定之納管對象：7,689個(110年5月19日止)

公務機關

- 中央與地方機關(構)
- 公法人

(不含軍事機關及情報機關)

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

機關類型	A級	B級	C級	D級	E級	總數
中央機關	43	145	336	318	111	953
地方政府	0	104	528	4987	684	6303
公法人	1	1	8	0	1	11
特定非公務機關	46	122	145	91	18	422
全部類型	90	372	1017	5396	814	7689

資安維護計畫實施情形

108、109年機關資安維護計畫實施情形

◘ 公務機關108年、109年資通安全維護計畫實施情形-應辦事項中未完成率較高項目

108年	A級公務機關	B級公務機關	C級公務機關
	1.資安職能評量**證書**	1.資安職能評量**證書**	1.資安專業**證照**
	2.資安專責**人員**	2.政府**組態基準**	2.資安職能評量**證書**
	3.一般使用者及主管資安**通識教育訓練**	3.資安專責**人員**	3.資安專責**人員**

109年	A級公務機關	B級公務機關	C級公務機關
	1.資安職能評量**證書**	1.資安職能評量**證書**	1.資安專責**人員**
	2.資安專責**人員**	2.資安專責**人員**	2.資安專業**證照**
	3.資通系統分級及**防護基準**	3.政府**組態基準**	3.資安職能評量**證書**

- 108年資料不含司法院所屬機關及公立高中職以下學校
- 109年資料不含司法院所屬機關

資安專責人員、資安專業證照、職能評量證書為主要未完成項目

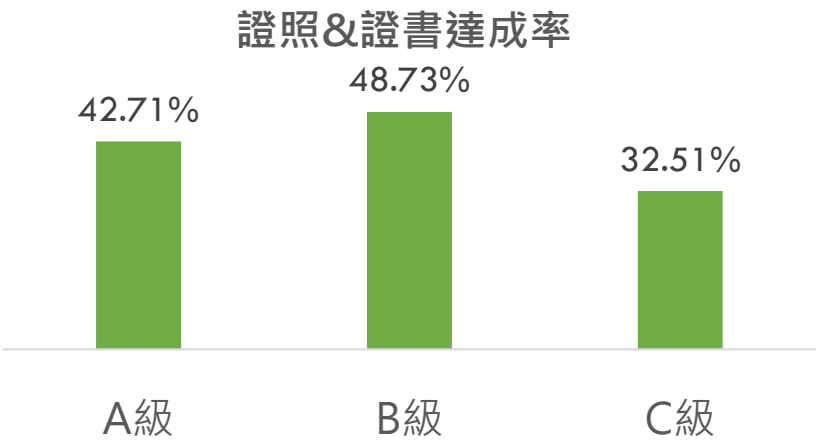
108、109年機關實施情形-資安專責人員

◘A、B、C級機關資安專職人員配置及持有資通安全專業證照及資通安全職能評量證書符合情形

108年

	法定人數	達成率
A級	4人	62.79%
B級	2人	60.08%
C級	1人	53.85%

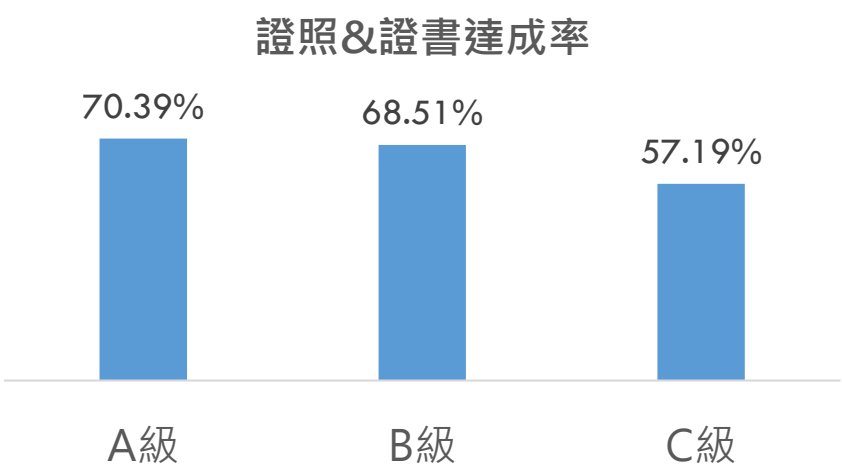
註：截至109年6月30日



109年

	法定人數	達成率
A級	4人	77.27%
B級	2人	66.80%
C級	1人	56.80%

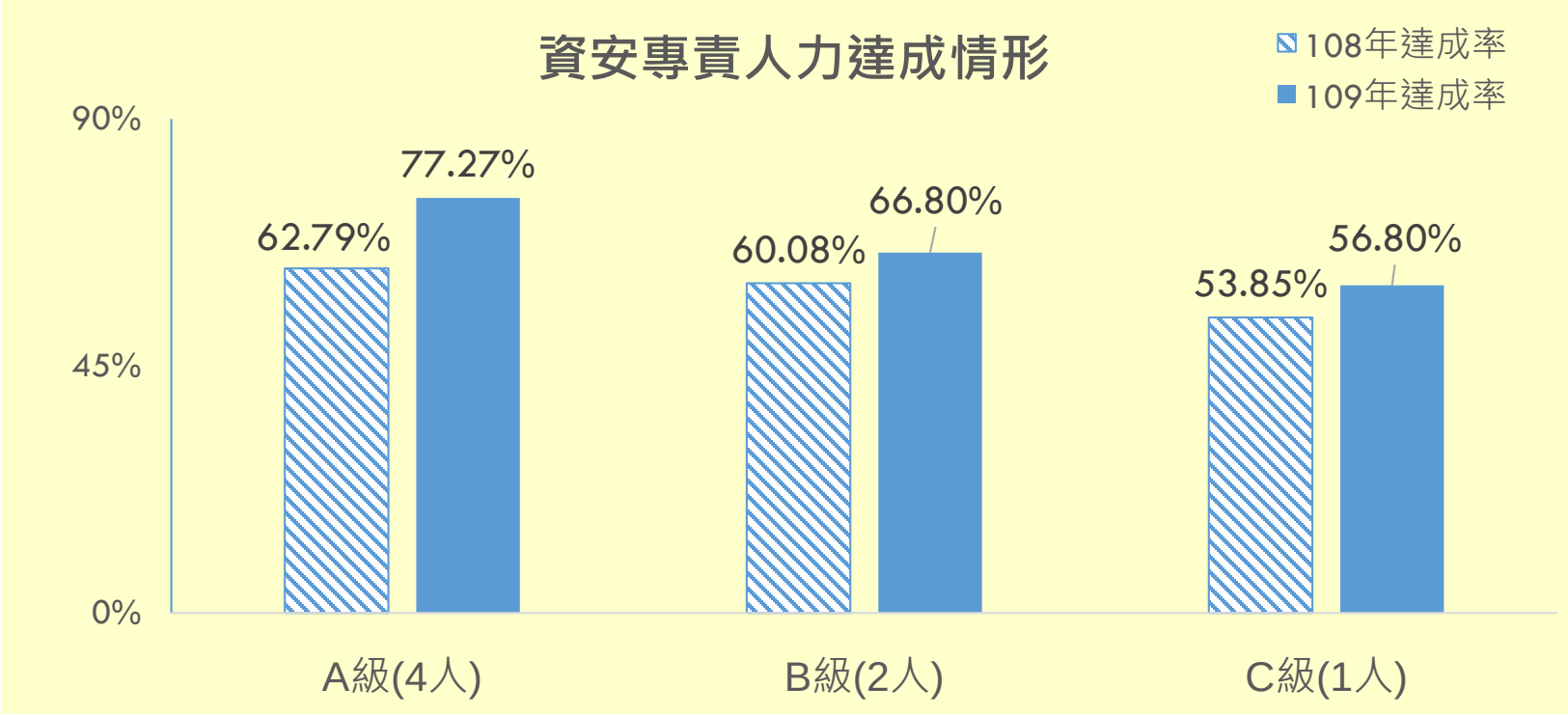
註：截至110年5月19日



機關實施情形-資安專責人員

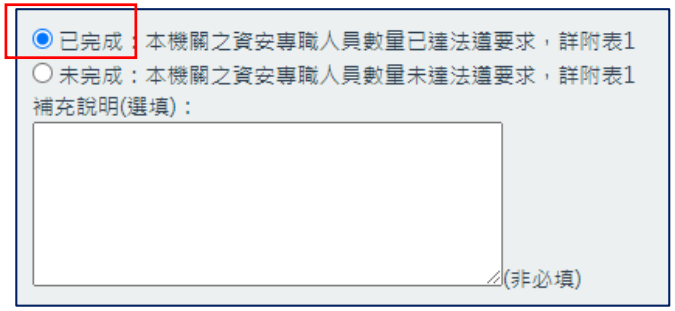
◘A、B、C級機關資安專職人員配置情形

- 如暫無員額配置，得先以約聘僱或委外人員擔任
- 適時減併資通系統，並評估向上集中：由上級機關統籌資通訊及資安作業與資源



機關實施情形-填寫常見問題

- 「資通系統及服務資產清冊」並非僅盤點自行建置、維運、管理的系統，而是針對機關所「使用」的系統進行盤點(含主管/上級機關提供)，俾機關及主管(上級)機關掌握其使用情形、重要性及資安防護等相關資訊
- 機關在填寫相關表單時，需注意是否有資料不一致的問題，如「附表1-機關專職人力」及「機關應辦事項」資料矛盾等情形(填寫人數低於要求但應辦事項填寫已完成)



附表3「資通系統及服務資產清冊」畫面參考

資通安全維護計畫實施情形-總結

- 資通安全專職人員配置及其專業證照、職能評量證書的取得仍為相對較常見之問題
- 各機關應成立或參與資安推動小組，每年定期辦理管理審查會議，檢視小組成員之資安法應辦事項辦理情形，如資安專職人力配置、機關及其所屬機關稽核、資通安全維護計畫檢討等事項，並追蹤改善情形，以持續精進落實防護作業，確實降低資安風險
- 若機關有部分系統無法導入GCB(政府組態基準)，針對不適用之項目應有相應替代作為(例外管理)，須注意例外管理之強度不宜太低，以確保其資安防護效果

資安事件通報

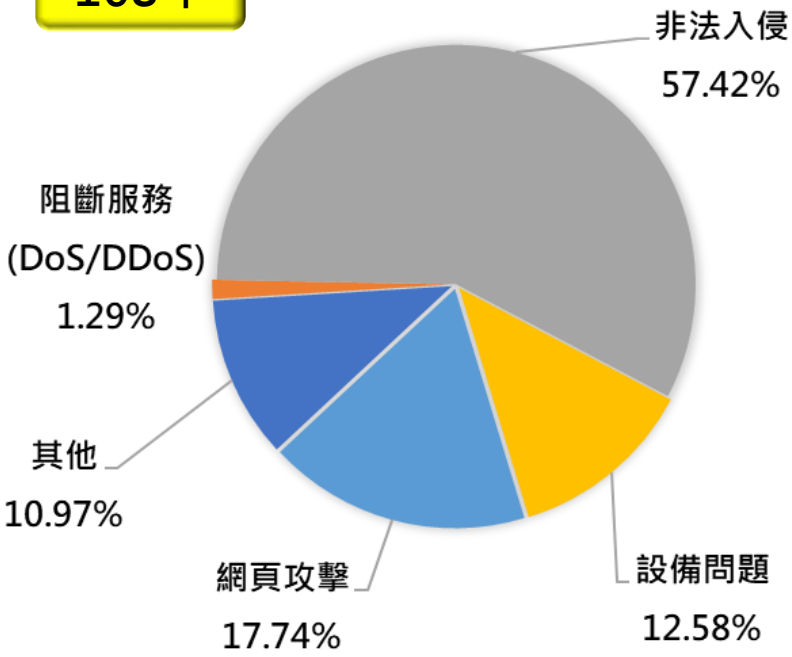
公務機關資安事件通報統計

年度	事件數	1級事件	2級事件	3級事件	4級事件
108年	310	254	45	11	0
109年	525	451	65	9	0

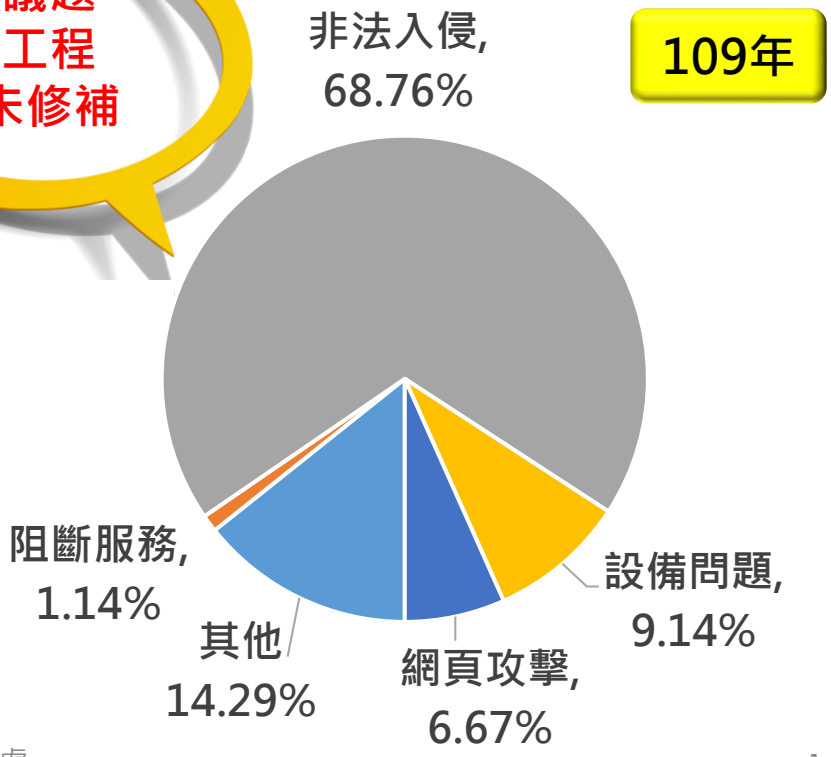
註：3級以上為重大資安事件
資安長應召開會議研商

密碼議題
社交工程
弱點未修補

108年

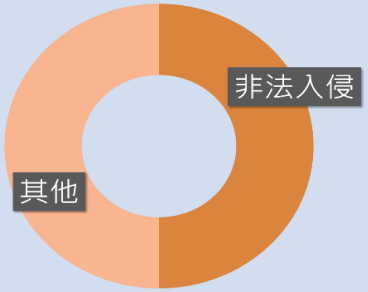
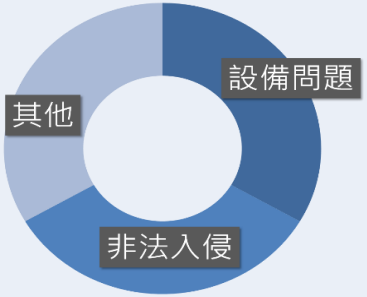


109年



公務機關109年重大資安事件

- 109年通報之資安事件，以收到技服中心資安警訊後通報為主，約占所有通報事件59.80%，機關自行偵測能量仍有待提升
- 109年9件3級資安事件通報，6件為資料外洩，3件為核心業務中斷

重大資安事件類型	發生原因	建議
資料外洩 	網站**設計不當**，導致網站具**漏洞**可存取敏感資料	應依弱點掃描、資安健診結果，**修補系統既有弱點**
	供民眾登記資料的表單**權限**設定**錯誤**，導致可被公開檢索與編輯	強化人員**資安意識**、**個資保護意識**宣導
	機關內部**人員疏失**，將含有敏感資料檔案**夾帶**於信件中寄出	
核心業務中斷 	機關遭非法入侵植入**勒索**軟體，因**無法**啟用**備援**機制，影響核心業務運作	訂定**異地備份**機制及**網路區隔**
	設備故障，影響涉及關鍵基礎設施維運之核心資通系統運作	訂定**備援機制**

納管機關事件通報及應變處理時效(1/2)

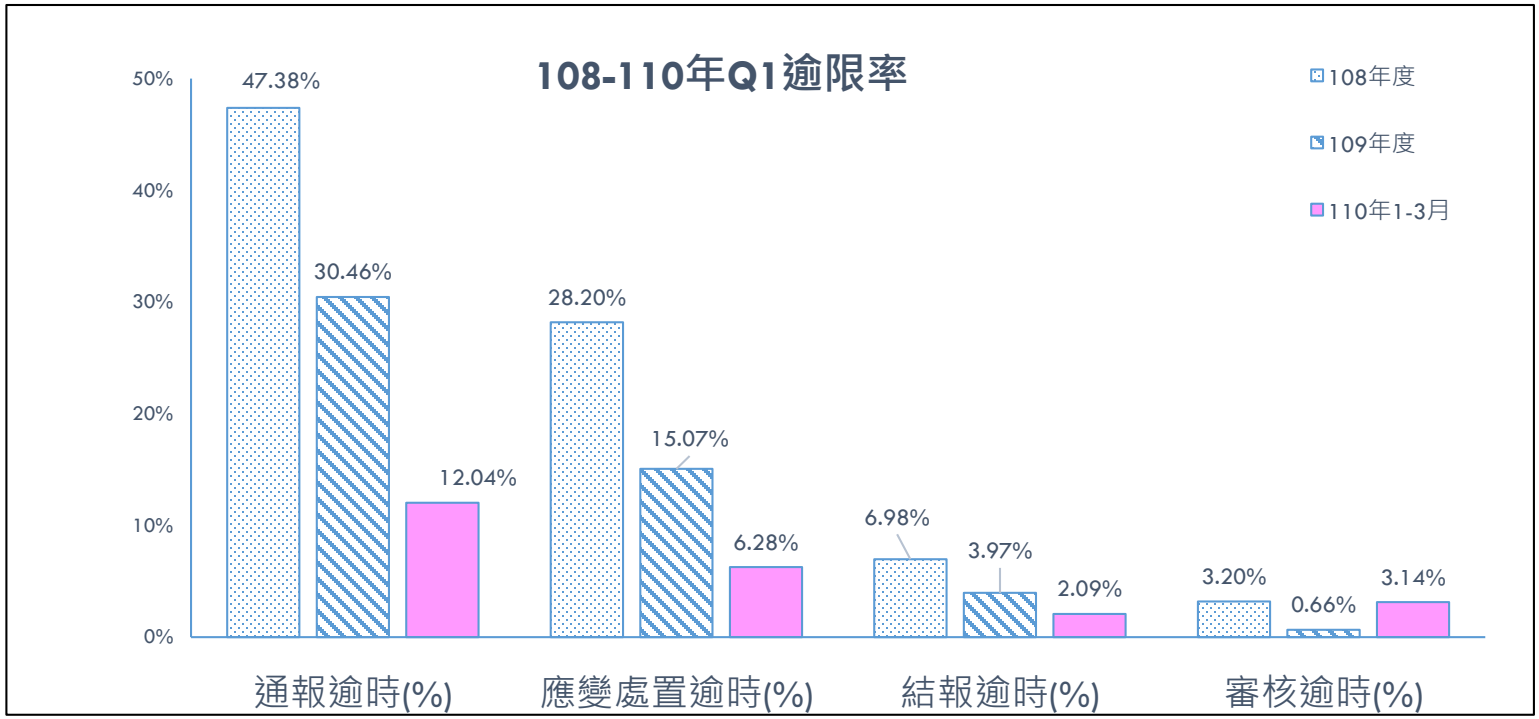
- 應依「資通安全事件通報及應變辦法」，於法遵時限內進行通報、審核、應變處置及結報
- 須注意事件通報需於知悉事件內1小時內通報，而非資安事件發生時間1小時內
- 每月統計逾限情形，提供當事機關及上級機關每季彙整提供上級機關、資安會報中提報

	事件通報	完成審核 (審核機關)	應變處置	結報 (提交調查、處理及改善報告)
起算時間點	知悉事件	接獲通報	知悉事件	完成應變處置
1、2級事件	1小時	8小時	72小時	1個月內
3、4級事件		2小時	36小時	

納管機關事件通報及應變處理時效(2/2)

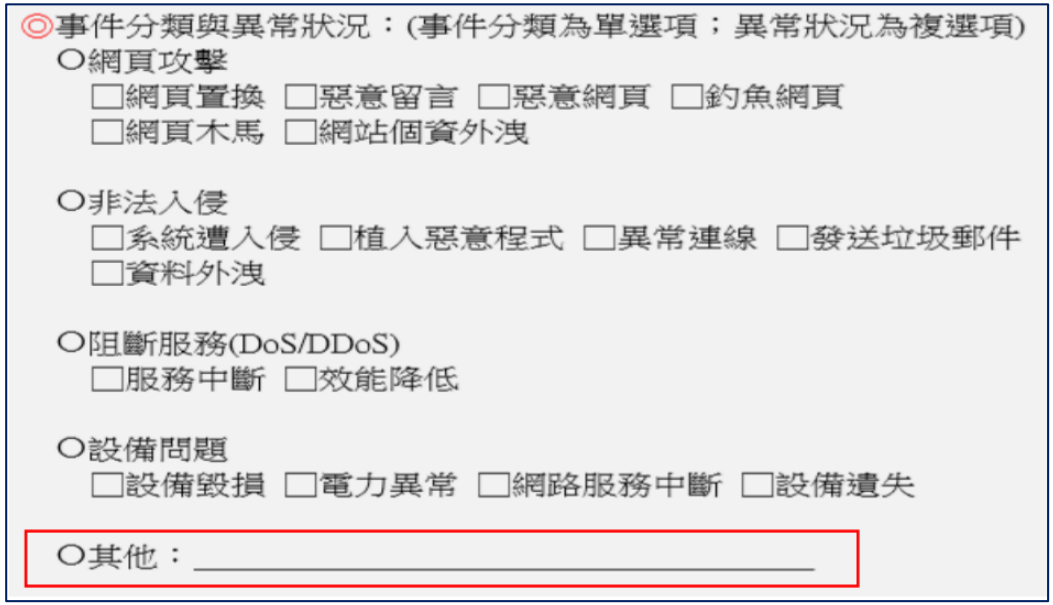
◘ 逾限原因

- ➢ 不熟悉通報流程→納入演練
- ➢ 認為無需通報→CIA受影響，不限被駭
- ➢ 資安目標為不發生資安事件→勿以資安事件數量為KPI



資通安全事件通報宣導(1/2)

- 知悉資安事件後，應至國家資通安全通報應變網站 https://www.ncert.nat.gov.tw，於時限內完成通報作業
- 通報填寫時，應確認資安事件的歸類，如勾選其他，則應敘明事件類型，俾主管(上級)機關及技服中心快速釐清事件並提供相關協助


◎事件分類與異常狀況：(事件分類為單選項；異常狀況為複選項)
○網頁攻擊
□網頁置換 □惡意留言 □惡意網頁 □釣魚網頁
□網頁木馬 □網站個資外洩

○非法入侵
□系統遭入侵 □植入惡意程式 □異常連線 □發送垃圾郵件
□資料外洩

○阻斷服務(DoS/DDoS)
□服務中斷 □效能降低

○設備問題
□設備毀損 □電力異常 □網路服務中斷 □設備遺失

○其他：_____

資通安全事件通報宣導(2/2)

- 事件說明及影響範圍應儘量完整
  - 機關發現資安事件的時間
  - 機關如何確認資安事件(如清查主機目錄)
  - 處理方式(如通知系統維護廠商、暫停系統服務等)
  - 估計影響範圍(受影響的是硬體或資通系統、影響哪些單位及機關等)

◎事件說明及影響範圍

【請說明事件發生經過，如機關如何發現此事件、處理情形等】

資安稽核作業

資通安全稽核作業

01 內部稽核(非僅資訊單位)

A級：每年2次
B級：每年1次
C級：每2年1次

02 對所屬機關稽核

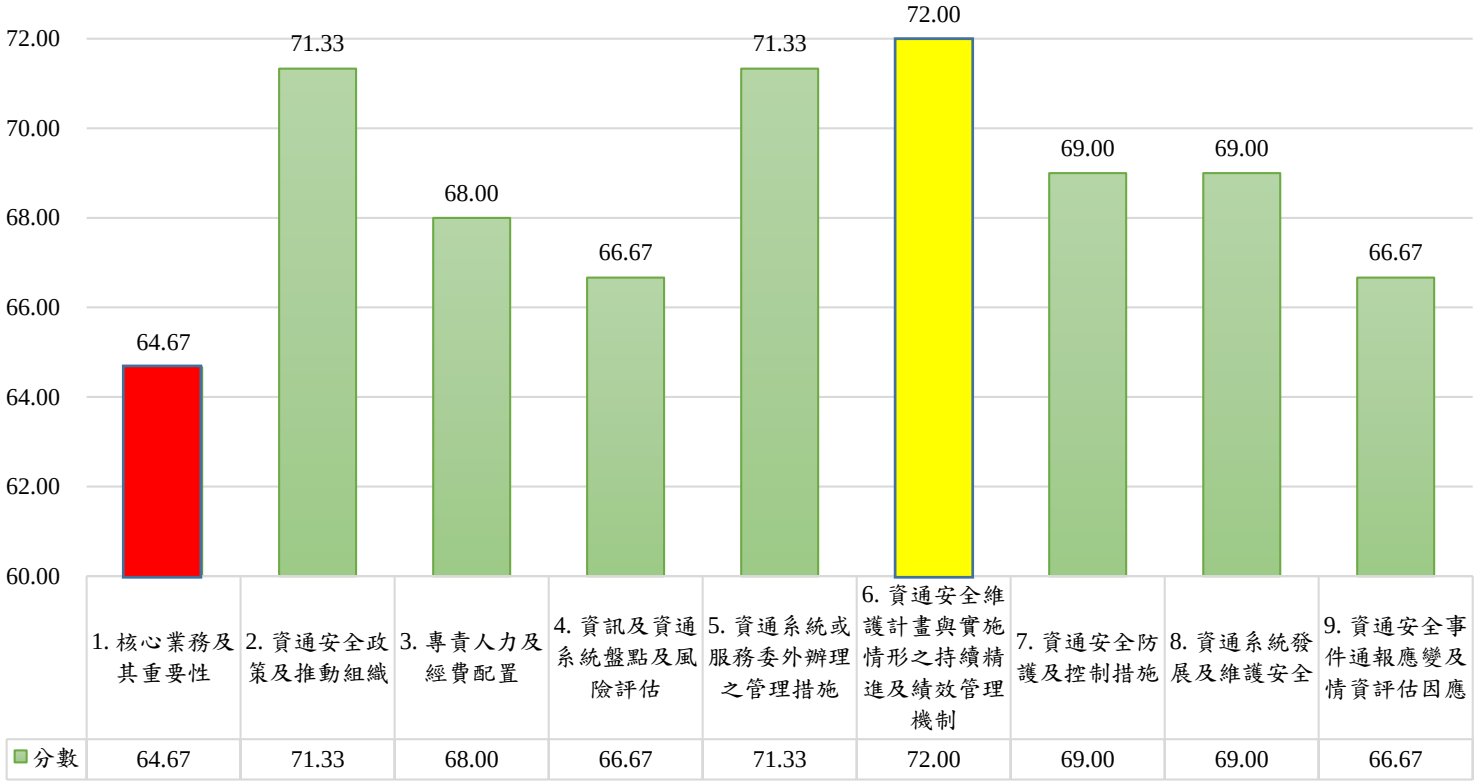
- 稽核計畫
- 資安維護計畫實施情形
- 稽核項目檢核表及評分表

03 對特定非公務機關稽核

- 所管特定非公務機關資通安全作業管理作業辦法
- 稽核結果送主管機關備查

資安稽核結果公務機關整體表現(1/2)

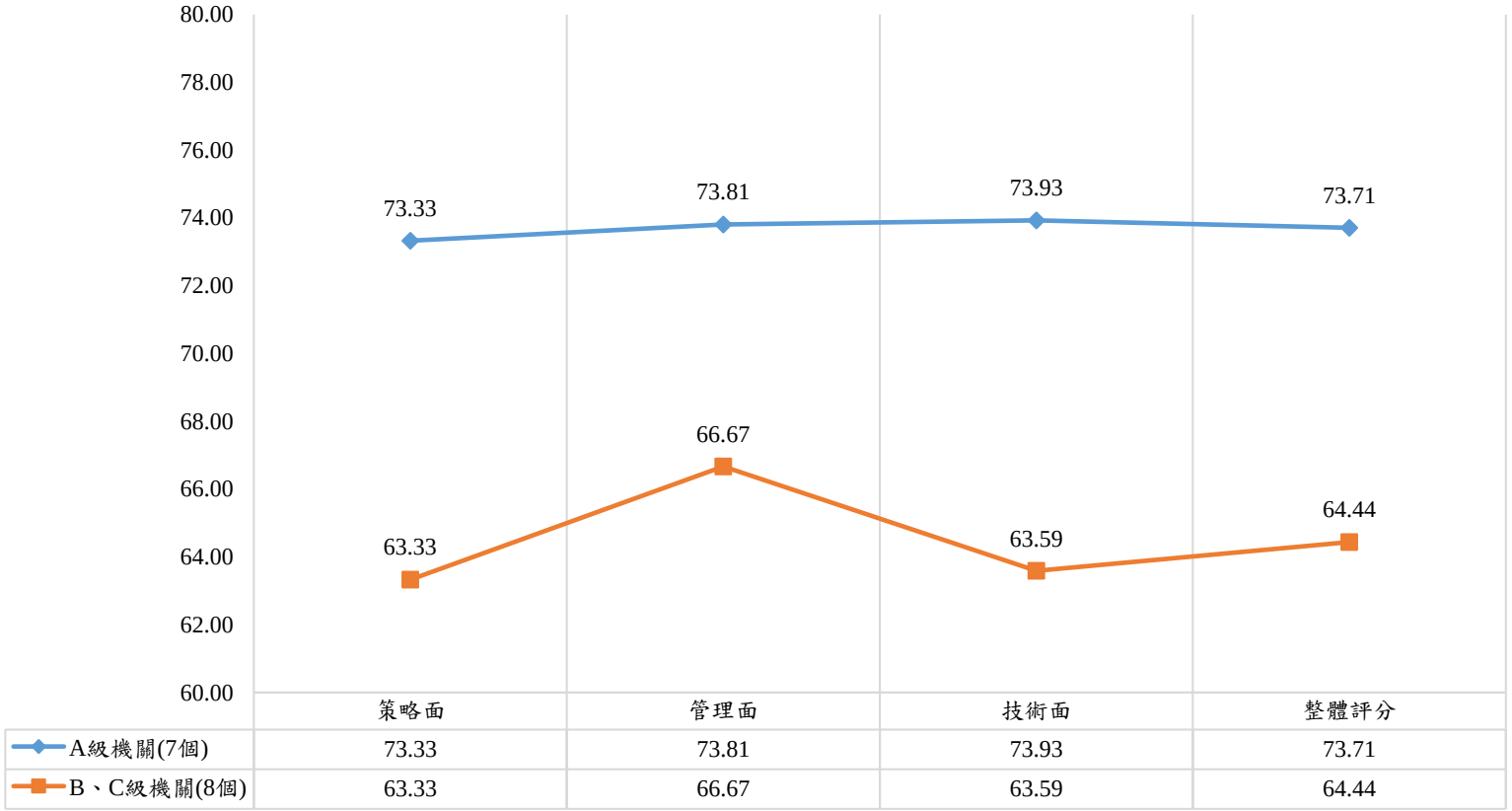
稽核個別項目成績



- 「資通安全維護計畫與實施情形之持續精進與績效管理機制」表現最好，顯示機關已重視資安防護，由資安長帶領推動組織制定、實施、檢討及精進資通安全維護計畫
- 「核心業務及其重要性」成績最低，顯示部分機關對核心資通系統之識別及資安防護仍待強化

資安稽核結果公務機關整體表現(2/2)

依資通安全責任等級區分

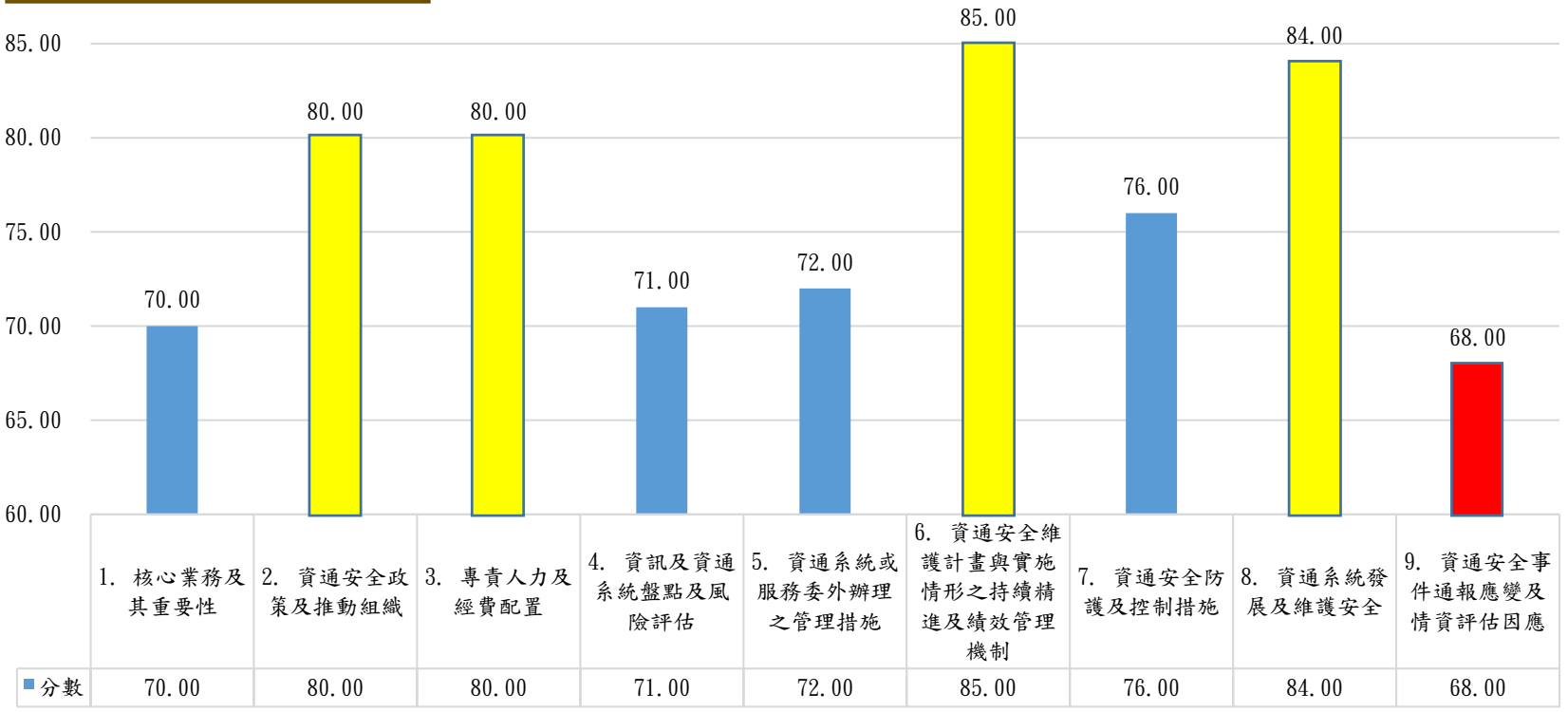


	策略面	管理面	技術面	整體評分
A級機關(7個)	73.33	73.81	73.93	73.71
B、C級機關(8個)	63.33	66.67	63.59	64.44

- A級公務機關在各構面均明顯優於B、C級公務機關
- A級機關各構面能平衡發展，且平均分數皆達73分以上，普遍表現尚可；B級機關各構面項目實施結果尚待加強

資安稽核結果特定非公務機關整體表現(1/2)

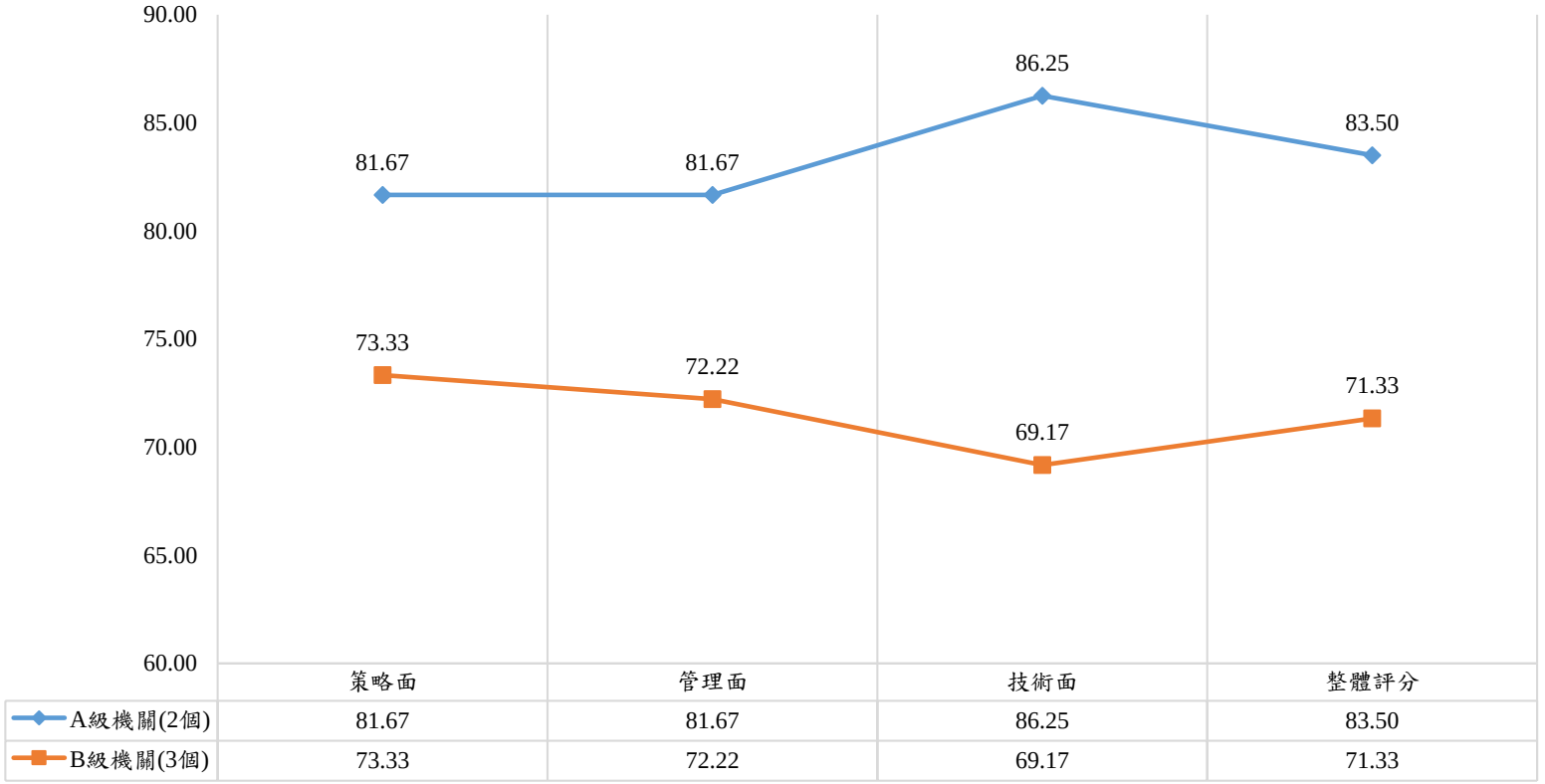
稽核個別項目成績



- 「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」、「資通系統發展及維護安全」、「資通安全政策及推動組織」及「專責人力及經費配置」等4項表現良好，平均分數均達80分以上
- 「資通安全事件通報應變及情資評估因應」平均分數低於70分，顯示資安事件之通報應變及情資分享機制仍待強化

資安稽核結果特定非公務機關整體表現(2/2)

依資通安全責任等級區分



	策略面	管理面	技術面	整體評分
A級機關(2個)	81.67	81.67	86.25	83.50
B級機關(3個)	73.33	72.22	69.17	71.33

- A級特定非公務機關在各構面明顯優於B級特定非公務機關，且平均分數皆達80分以上，普遍表現良好，B級機關表現尚可

109年稽核共同發現事項

策略面

- **核心業務**與**核心資通系統**未**有效界定**
- **利害關係人**未完整建立並定期檢視
- 維護計畫與**實施**情形有**落差**
- **資安**專責**人力**未能依法配置

管理面

- 資訊**資產盤點**及資產清冊，**範圍**與**內容**完整性**不足**
- **委外作業**未依法**明確**規劃與**落實**
- **內稽未涵蓋全機關，稽核項目未完整納入應辦事項**

技術面

- **網路架構**安全性仍顯不足，如網段區隔、存取控制
- **安全性檢測**與**資安健診**待加強，**改善追蹤**未確實
- 資通**系統**安全**開發**尚**未**納入資通系統**防護需求**
- 資安事件通報及應變**演練**，**未納**入事件**通報**；另建議演練情境納入**新興**資安**議題**或事件

109年第二方稽核輔導

- 為落實資安分層管理監督之精神，實施輔導第二方稽核作業，提供予上級/監督/中央目的事業主管機關稽核所屬/所監督/所管之機關時參考
- 第二方稽核輔導作業，安排專家協助檢視受輔導機關所提稽核文件，並現場觀察受輔導機關對受稽核機關之實地稽核
- 第二方稽核輔導以3個階段進行
  - 提供稽核範本：包含資安稽核相關文件與表單之範本，機關可依受稽核機關之屬性、應遵循法規及資安維護要求等加以調整，發展為其自有之第二方稽核作業
  - 諮詢服務：提供受輔導機關辦理第二方稽核相關之諮詢服務，並彙整常見問題供參考
  - 文件檢視與實地輔導：檢視第二方稽核相關文件(例如稽核計畫、稽核檢核表、稽核評分表、稽核報告表單、啟始/結束會議簡報等)之妥適性

109年第二方稽核輔導共同建議

稽核規劃

- 將**核心業務**與資通**系統**納入稽核範圍
- 計畫應納稽核**追蹤改善**方式
- 適當配置**稽核重點**、面向及**委員**人數

稽核實施

- **啟始**會議簡要**說明**稽核重點，如時程、範圍、準則、地點及保密等，俾**受稽人員了解**
- 啟始會議提供**受稽機關簡報**，俾**稽核委員**快速**掌握**受稽機關之資通安全防護作為

稽核委員

- 稽核委員**培訓**：強化稽核**抽樣**與軌跡**追蹤**
- 應了解稽核**項目**之**準則**要求，俾查核落實
- **委外管理**應關注廠商**遴選**、服務交付及**監督**之過程

稽核結果

- 稽核發現彙整，應**統一**優點與待改善之**語法**
- **稽核報告**內容應於**結束會議前**予以**確認**
- 稽核報告應納入稽核目標、受稽機關、稽核團隊、日期、地點、稽核準則聲明及結論等

攻防演練

109年社交工程演練結果(1/2)

- 透過「社交工程演練系統」，隨機寄發郵件或簡訊，記錄使用者「郵件開啟」、「郵件附件/連結點閱」及「簡訊連結點閱」等行為

	受測人數	郵件開啟率	檔案/連結點閱率
郵件	11,448	6.66%	4.27%
簡訊	1,259	-	25.66%

郵件開啟裝置	開啟比例	檔案/連結點閱比例
桌機	5.61%	3.92%
行動裝置	0.74%	0.25%
桌機與行動裝置	0.31%	0.10%

109年社交工程演練結果(2/2)

- 近期惡意電子郵件攻擊所用議題越趨精準，為避免因瀏覽惡意電郵，影響網路安全、或致重要資訊外洩。有效提升公務人員對電子郵件的警覺性，108年起提升演練郵件的擬真程度，並增加及優化點閱率較高類別：公文類及財經類，如會議紀錄、收據、對帳單等
- 109年簡訊連結點閱率為25.66%，點閱簡訊連結的機關比例為69.49%，簡訊社交工程演練結果顯示，對於社交簡訊防範意識較為薄弱，資安意識仍需強化

109年資通系統實兵演練

- 5,289個資通系統，執行方式
  - 以不影響機關系統正常業務運作為原則
  - 模擬駭客實際攻擊演練機關之對外服務系統與網路，嘗試取得機關內部機敏資料或系統控制權限

排名	弱點類型	108年	109年
1	不安全的組態設定	16.8%	45.6%
2	無效的身分認證	20.8%	25.7%
3	無效的存取控管	22.1%	12.8%
4	跨網站腳本攻擊	17.3%	8.4%
5	注入攻擊	10.7%	4.9%
6	機敏資料外洩	10.9%	2.2%
7	使用已知漏洞元件	1.3%	0.4%

常見弱點類型及防護建議(1/3)

不安全的組態設定(45.6%)

- 網站之相關安全性設定參數設定錯誤或是安全防護強度不足，而導致如網頁可能暴露系統非公開資訊，或攻擊者可能透過瀏覽網站目錄，取得機敏資料，以及攻擊者可上傳後門程式獲取系統權限

改善建議

- 確實檢查網站相關安全性設定，如：對外顯示錯誤訊息功能、目錄瀏覽功能以及限制上傳檔案類型，並經過檔案驗證確認檔案類型之正確性等

常見弱點類型及防護建議(2/3)

- 無效的身分認證(25.7%)
  - 身分認證與session管理相關之功能未正確執行，導致攻擊者破壞身分認證機制，常見原因為密碼強度不足

- 改善建議
  - 建議刪除或停用預設帳號，再另行建立管理者帳號；若預設帳號無法更動則至少須修改預設通行碼
  - 通行碼建議具備高複雜度，同時禁止使用者設定與帳號相同之通行碼

常見弱點類型及防護建議(3/3)

◘ 無效的存取控管(12.8%)

- 網站未對每個頁面進行存取控制權限的要求，一般使用者只需知道網址位置或進行位址猜測，即可越權存取機敏資料或操作系統功能

◘ 改善建議

- 應對所有功能頁面進行權限控管，同時權限檢查須區分存取來源為使用者或管理者
- 所有檢查應於伺服器端進行，僅回傳必要之檢查結果，避免將未授權之功能頁面併入檢查結果中回傳，以防遭攻擊者竄改進而繞過檢查機制

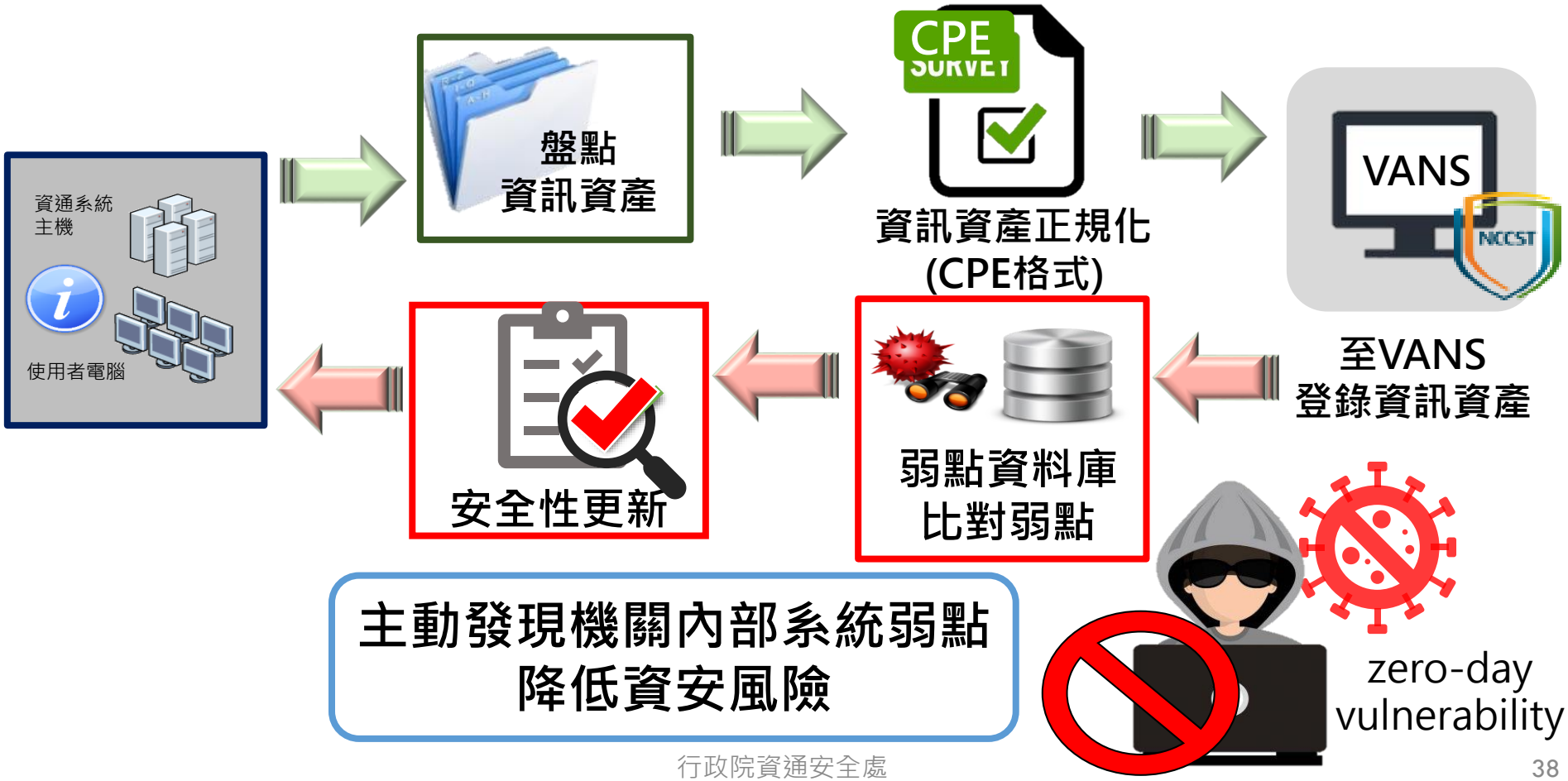
近期作業宣導

分級辦法技術面增修方向

納管對象 / 項目	A級、B級		C級	
	公務機關	關鍵基礎設施提供者	公務機關	關鍵基礎設施提供者
資安弱點通報機制(VANS)	初次受核定、等級變更或經主管機關發布後之**一年內**，完成資安弱點通報機制導入作業，並持續維運		初次受核定、等級變更或經主管機關發布後之**二年內**，完成資安弱點通報機制導入作業，並持續維運	
端點偵測及回應機制	初次受核定、等級變更或經主管機關發布後之**二年內**，完成端點偵測機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料	-	-	

政府機關資安弱點通報機制

- 結合資訊資產管理與弱點管理，將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊，並依風險情形完成安全性更新



資訊資產弱點管理流程

透過合作廠商工具產出CPE格式報表，並可透過API上傳至VANS系統

搭配廠商工具盤點

透過CPE模組轉換為CPE格式

透過系統指令或工具盤點

彙整資料

比對以轉換為CPE格式

上傳方式

手動上傳

資訊資產CPE清單

API上傳

由API上傳至VANS系統

手動上傳至VANS系統

資產管理

軟體

弱點管理

弱點通知

資訊綜整

資訊資產清單

機關概況

透過AD派送批次檔方式盤點軟體資產資訊，再以PowerQuery擴充套件彙整

VANS系統

端點偵測及回應機制(EDR)

- 端點偵測及回應機制(Endpoint Detection and Response, EDR)運作以agent(代理程式)掃描異常程式/行為，經過server分析後，以等級評分等方式呈現可疑程式之可疑指數與相關時序，並評估整體單位風險，並可偵測到規避防毒軟體的滲透攻擊(如離地攻擊)及防範其他未知威脅
- 以蒐集端點鑑識資料為主，大致包含
  - 主機資訊(基本資訊、網路組態、日誌等)
  - 惡意程式相關資訊(記憶體、活動歷程、特徵標註等)
  - 網路連線相關資訊(內外部網路連線)

EDR產品標準功能需求

- 以端點掃描查找可疑程式與異常活動
- 可列出可疑程式之威脅程度(以指數或等級表示)、判斷依據與其相關資訊(metadata)
- 具介面可呈現並查詢端點掃描結果與單位整體威脅情況
- 原廠持續提供技術協助與掃描資料判讀
- 後續應可配合匯出並提交偵測資料
  - 提供資料對外轉拋、介接功能或API可供利用
  - 可提供經分析後高風險樣本或事件相關資訊

強化委外契約管理(1/2)

- 建議機關採用工程會110年4月9日發布新版「資訊服務採購契約範本」，其資安相關修正內容摘要如下
  - 第二條 履約標的，廠商如提供資訊業務線上服務，應於服務建議書向機關敘明資通安全管理機制及防護措施
  - 第八條 履約管理，明確訂定廠商及其分包廠商之責任，限制執行團隊不得有陸籍人士，並不得提供及使用大陸廠牌資通訊產品
  - 第十五條 違約及服務績效違約金，將資安事件通報應變、資料外洩或遭竄改列入資安指標
  - 第十六條 權利及責任，授權資通安全管理法主管機關得稽核廠商(含分包廠商)，並適度公開資安事件內容；另明確訂定廠商責任
  - 第十八條 契約終止、解除及暫停執行，因資安致使機關遭受嚴重損害者，機關得終止、解除及暫停執行契約
- 建議各類財物、勞務、工程採購，如涉資通系統或服務，亦應參考資訊服務採購契約範本內容，納入相關規定

強化委外契約管理(2/2)

- 加強委外廠商服務期間之資通安全監督與管理
- 要求廠商遵循主管機關訂定之標準或規範執行，並提供可行建議方案，確保委外作業安全，例如
  - 委外廠商之應用系統開發環境是否安全，是否納入SSDLC，程式測試資料是否合宜等
  - 測試機與正式上線系統網段是否進行區隔
  - SOC監控委外蒐集之資料是否做好相當之管理及防護
- 如配置駐點人員，應要求該人員遵守資安法相關規範及機關內部資安管理機制
- 機關採購單位、總務單位可能未知悉契約須納入資安相關要求，爰請資訊單位協助提醒業務單位在計畫審查或採購案會辦時，將資安要求納入各類契約內，建議相關規定可以提報機關資安管審會，讓資安長知悉，並周知所有單位配合辦理

各機關資通安全事件通報及應變處理作業程序

- 事件通報及應變小組：指揮官、情資及計畫組、應變執行組、後續調度組
- 3、4級資通安全事件，各機關除規定通報外，應另以電話通知上級機關或中央目的事業主管機關

事件通報

- 3、4級資通安全事件，資安長應召開會議研商相關事宜

1.資通安全事件概況
2.評估受影響範圍
3.其他必要之討論事項

事件應變會議

1. 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形
2. 評估是否對外公告
3. 依規定完成通知作業

損害控制或復原措施

建議項目(6個月)
1.作業系統日誌
2.網站日誌
3.應用程式日誌
4.登入日誌

TWCERT/CC
https://viruscheck.tw/

- 除設備故障外，應保存跡證，督導進行根因調查，並提出紀錄分析；若發現惡意程式，應上傳Virus Check檢測，並送防毒或資安公司檢測
- 評估短、中、長期資安管理改善策略

根因分析

1. 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形
2. 評估是否對外公告
3. 依規定完成通知作業

改善追蹤

勿採購或使用大陸廠牌產品

- 大陸廠牌：以廠牌為認定，無論產地為何；包含貼牌
- 資通訊產品：依資通安全管理法第3條名詞定義，包含軟體、硬體及服務等項，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品

公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。

個人資通訊設備不得處理公務事務，亦不得與公務環境介接。

各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

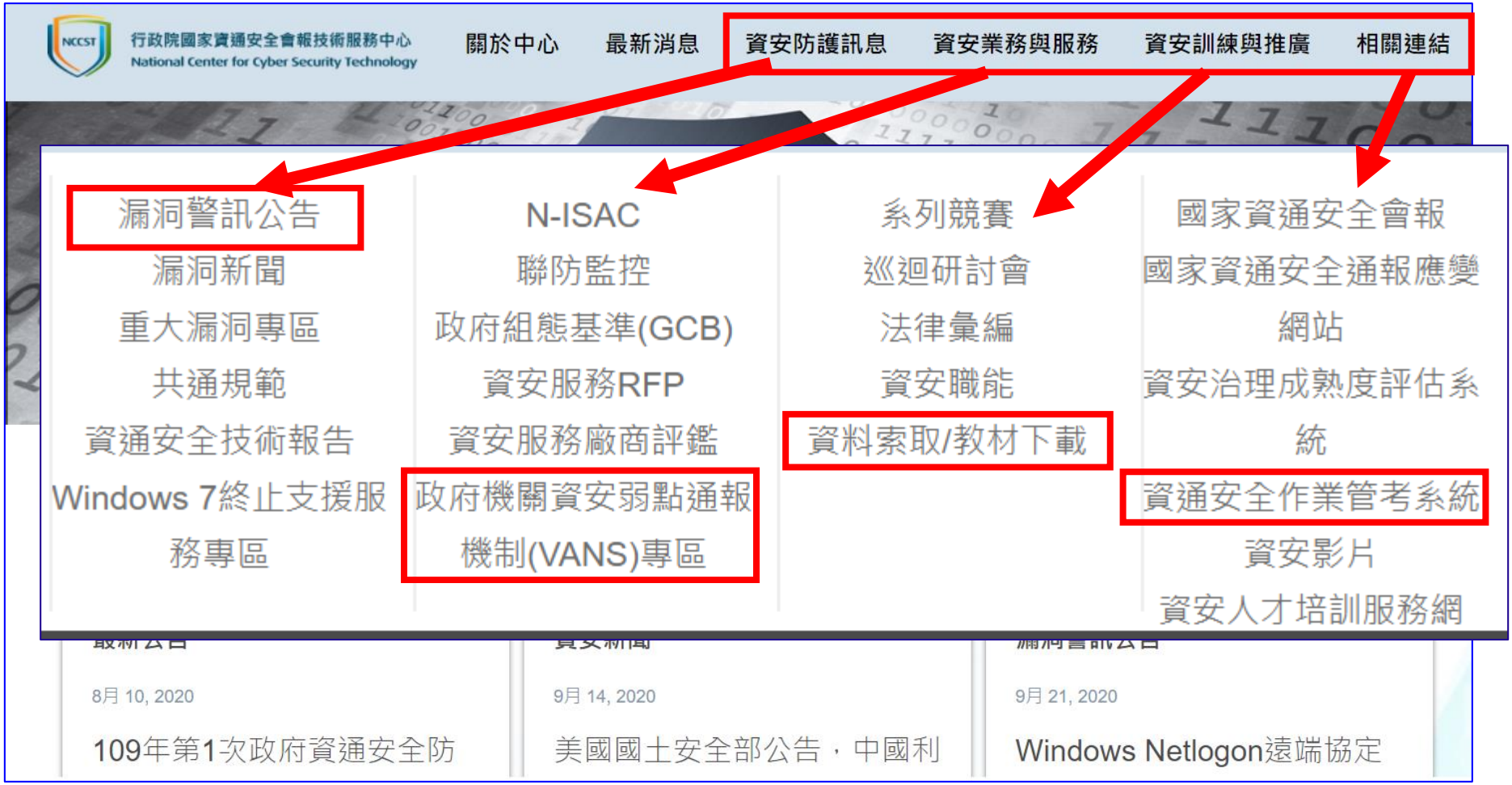
行政院資安處109年12月18日院臺護長字第1090201804A號函

參考資訊

- 行政院國家資通安全會報 https://nicst.ey.gov.tw/

參考資訊

- 技術服務中心 https://www.nccst.nat.gov.tw/



資安是持續精進的風險管理