資通安全管理法
施行情形說明

行政院資通安全處

109年5月

大綱

一、前言

二、108年資通安全維護計畫實施情形

三、108年資通安全事件通報情形

四、108年網路攻防演練辦理情形

五、108年資通安全稽核執行成果

六、總結

一、前言

前言

- 資通安全管理法自108年1月1日開始實施
- 納管對象為公務機關與特定非公務機關
  - 公務機關：中央、地方機關(構)或公法人，但不包括軍事機關及情報機關
  - 特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人
- 截至108年4月30日，資安法納管機關數量及各資安責任等級核定數量如下：

機關類型	A級	B級	C級	D級	E級	總數
全部類型	54	275	1,153	5,284	783	7,549
中央機關	44	144	372	301	112	973
地方政府	0	113	673	4,900	651	6,337
特定非公務機關	10	18	108	83	20	239

二、108年資通安全維護計畫實施情形

資通安全維護計畫實施情形

依據

- 資通安全管理法第12條、第13條、第16條及第17條

目的

- 依資通安全管理法規定，檢視機關資通安全維護計畫實施情形。
- 使上級機關確認所屬機關實施成效，了解及稽核所屬或受監督機關之年度資通安全維護情形

應辦事項

- 依資安法第十二條公務機關應每年向上級機關提出資通安全維護計畫實施情形。機關應研擬資通安全維護計畫，可與上級機關合併計畫
- 每個機關(A~E級)都要提報實施情形

資通安全維護計畫實施情形-背景介紹

- 109年2月24日發函至各機關，完成108年資通安全維護計畫實施情形提報作業
- 至行政院資通安全會報資通安全作業管考系統(https://spm.nat.gov.tw/)進行實施情形的填報

資通安全維護計畫(1/3)

一、核心業務及其重要性
- **核心業務及重要性盤點**

二、資通安全政策及目標
- **資通安全政策訂定及核定**
- **資通安全目標之訂定**
- **資通安全政策及目標宣導**
- **資通安全政策及目標定期檢視**

三、資通安全推動組織
- **設置資通安全推動小組**

四、專責人力及經費之配置
- **專職(責)人員配置***
- **經費之配置***

五、公務機關資通安全長之配置
- **設定資通安全長**

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產
- **資訊及資通系統之盤點***
- **機關資通安全責任等級分級**

七、資通安全風險評估
- **資通安全風險評估**
- **資通安全風險之因應**

註：紅字底線項目為完成度較低項目

資通安全維護計畫(2/3)

八、資通安全防護及控制措施

- **資通安全防護及控制措施**
- **資訊及資通系統之保管**
- **存取控制與加密機制管理**
- **作業及通訊安全管理**
- **系統獲取、開發及維護**
- **業務持續運作演練**
- **執行資通安全健診**
- **資通安全防護設備**

九、資通安全事件通報、應變及演練相關機制

- **訂定資通安全事件通報、應變及演練相關機制**
- **資通安全事件通報、應變及演練**

十、資通安全情資之評估及因應機制

- **資通安全情資之分類評估**
- **資通安全情資之因應措施**

資通安全維護計畫(3/3)

十一、資通系統或服務委外辦理之管理措施。

- **選任受託者應注意事項**
- **監督受託者資通安全維護情形應注意事項**

十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

- **資通安全教育訓練要求**
- **辦理資通安全教育訓練**
- **訂定考核機制並進行考核**

十三、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。

- **資通安全維護計畫之實施**
- **資通安全維護計畫實施情形之稽核機制**
- **資通安全維護計畫之持續精進及績效管理(內稽)**
- **對所屬/所監督/所管機關(構)訂定稽核計畫**
- **對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核**

註：紅字底線項目為完成度較低項目

108年管考系統實施情形填報狀況

□資安維護計畫實施情形，各機關自評結果：

- 機關的平均達成率約為98%(未逾限)
- 1-2%項目逾限辦理
- A級機關中，實施情形自評項目完成率近95%，表現最佳

	已完成 未逾限	辦理中 未逾限	已完成 已逾限	辦理中 已逾限
A級機關	94.76%	4.29%	0.63%	0.32%
B級機關	88.28%	10.21%	0.42%	1.09%
C級機關	82.23%	15.49%	0.70%	1.60%
D級機關	88.69%	9.35%	1.00%	0.96%
E級機關	91.51%	6.68%	1.03%	0.78%

108年管考系統實施情形填報狀況

□35項實施情形，逾限且未完成率相對較高的項目：

除資安專職人力、資安推動小組外，稽核相關作業是機關未完成較高之項目。

序號	項目	未完成比例
1	資通安全維護計畫之持續精進及績效管理**(內稽作業)**	3.06%
2	**專職(責)人員**配置	2.65%
3	**對所屬/所監督/所管**機關(構)訂定**稽核計畫**	2.56%
4	設置**資通安全推動小組**	2.5%
5	資通安全維護計畫實施情形之**稽核機制**	2.48%
6	**對所屬/所監督/所管**機關(構)辦理資通安全維護計畫實施情形之**稽核**	2.36%

資安專責(職)人員配置

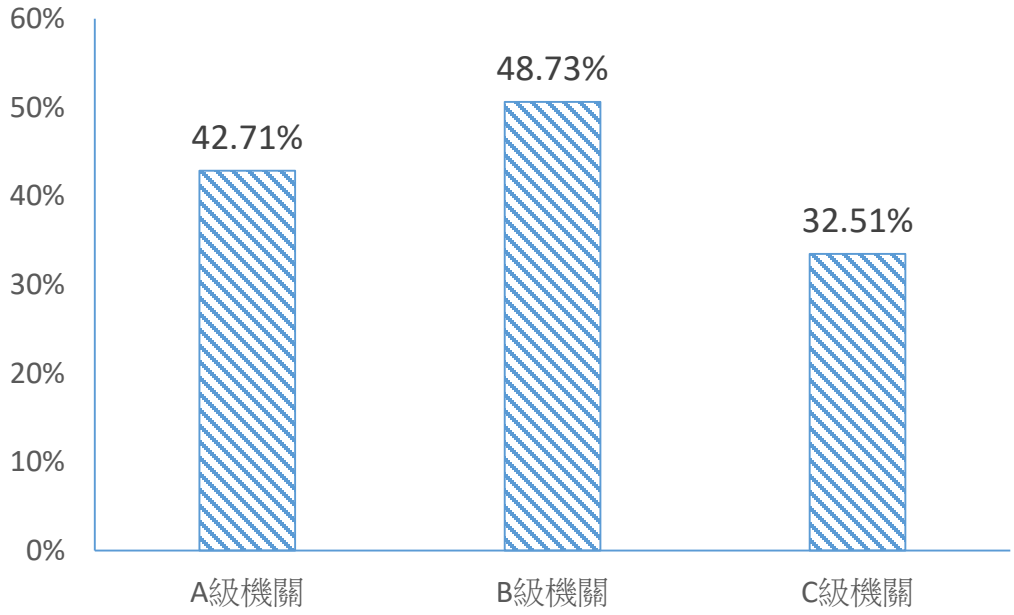
◘自評情形：

➢A、B、C級機關資安專職人員配置達成情形：

	專責(職)人員數目要求	人員配置要求達成率
A級	4人	62.79%
B級	2人	60.08%
C級	1人	53.85%

資安專職人力要求-證照及證書達成率

- 初次受核定或等級變更後之1年內，資通安全專責人員每人應持有1張以上資安專業證照及1張以上資安職能評量證書。
- 資安專職人員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：



資安專職(責)人員配置-辦理情形範例

~~已完成，未逾限~~	本機關108年依規定配置資通安全專責人員2人，其中專職人員1人，已具備資通安全專業證照1張及資通安全職能評量證書1張，詳如附表1。

公務機關資安專責人員應以專職人員配置

~~已完成，未逾限~~	本機關108年依規定配置資通安全專責人員1人，其中專職人員1人，已具備資通安全專業證照0張及資通安全職能評量證書0張。

資通安全專職人員每人需至少有一張以上專業證照及一張以上職能評量證書，**故本項應屬未完成。**

已完成，未逾限	本機關之業務經主管機關核定後之資通安全責任等級為D級，毋須配置資通安全專職人員。

D級、E級機關無資安專責人員配置需求

已完成，未逾限	本機關108年依規定無應配置資通安全專責人力要求，惟仍依現況設兼辦人員1人。

資安專職(責)人員配置-建議

- 資安法施行後，各機關應優先於機關總員額配置資安專職人力，惟為解決機關人力短時間調配之問題，如暫無缺額人力可支配，可先以約聘僱或委外人員擔任，至本法施行 2 年後，再以正式人員配置。
- 建議資訊業務規模小之機關可考慮將資通系統及資源向上集中，由上級機關統籌辦理，減少機關自行維運之負擔。

設置資通安全推動組織-自評及範例

- 約2.5%的機關，未設置或加入其他機關的資安推動小組。

已完成，未逾限	本館108年已設置資通安全推動小組，由[　　]擔任召集人，包含6個機關單位共6人，各單位成員層級為單位主管以上，其運作及成員職掌已訂於「[　　]資通安全維護計畫」第伍章第二點內。108年每季召開4次小組會議，由[　　]主持，成員親自出席比例為100%。

也可加入其他機關的資安推動小組及參加會議

~~已完成，未逾限~~	本總隊因資訊業務單純且規模小，僅維持基本資訊運作，未成立推動小組。

每個機關都應成立或參加其他(上級)機關的資通安全推動小組

維護計畫及實施情形之精進及績效管理機制

- 自評情形：
  - 約3.06%的機關，沒有訂定機關的資通安全維護計畫之持續精進及績效管理機制
  - 約2.48%的機關，沒有訂定資通安全維護計畫實施情形之稽核機制
- 建議：
  - 資安推動小組每年應定期開會，確認機關資安維護計畫之實施情形，持續精進以確保其適切性、合宜性及有效性。
  - 機關應每年執行稽核作業，檢視對規範遵循與管理程序要求的落實情形，確認資安作業的有效性。

維護計畫及實施情形之精進及績效管理機制-辦理情形範例

◘資通安全維護計畫之持續精進及績效管理

已完成，未逾限	本站稽核機制已訂定於資通安全維護計畫內，稽核項目已納入資通安全管理法相關規定，執行情形載明於資訊安全內部稽核管理要點文件，並透過管理審查會議定期檢核其執行情形。本站內部稽核對象共有6個單位，稽核規劃為每年6個，預於1年內可完成全部單位稽核。稽核小組成員包含6個單位，共6人，每次稽核成員規劃為每組室各指派1員參加。

◘資通安全維護計畫實施情形之(內部)稽核

已完成，未逾限	由上級機關　　每年度實施二次資訊內部稽核暨公務機密維護檢查，108年　　於7月3日及11月21日辦理稽核。

機關稽核機制可配合上級機關辦理

已完成，未逾限	108年於12月16及17日辦理1次內部稽核，計11個單位受稽，計有3項改善建議，已完成改善

已完成，未逾限	本分處上級機關於108年度至本分處進行稽核；計有5項改善建議，本分處已於108年11月前完成改善。

機關稽核機制可配合上級機關辦理

對所屬機關稽核與管理

- 自評情形：
  - 約2.56%的機關未訂定對所屬/所監督/所管機關(構)的稽核計畫
  - 約2.36%的機關未辦理對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核
- 建議：
  - 對所屬機關之稽核計畫，可參考本院109年資通安全稽核計畫，包含受稽機關之稽核周期、挑選原則、稽核小組成員規劃及後續問題追蹤機制等。

對所屬機關稽核與管理-辦理情形範例

◘ 對所屬/所監督/所管機關(構)訂定稽核計畫

不適用	無所屬機關

若無所屬機關，填不適用

已完成，未逾限	本機關所屬/所監督/所管機關(構)訂定稽核計畫配合「　　局108年資訊安全稽核實施計畫」，稽核項目已納入資通安全管理法相關規定，並透過「資訊稽核改善事項辦理情形」定期檢核執行情形。 本機關所屬/所監督/所管機關共有11個，稽核規劃為每年11個。 每次稽核小組成員包含2個單位，共2人。

可配合上級機關訂定的稽核計畫，稽核所屬機關

◘對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核

已完成，未逾限	本署108年已於108年7月辦理1個所屬機關之稽核作業，計有19項改善建議，已於108年10月18日前完成改善。

資通安全維護計畫實施情形-總結

- 多數機關自評已完成其資通安全維護計畫應辦與應遵守事項。
- 機關之資通安全維護計畫可併同其他機關共同擬定，但實施情形應由各機關自行向上級機關提報，上級機關應稽核所屬機關實施情形。
- 各機關應成立或參與資安推動小組，每年定期召開管理審查會議，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。
- 機關應依法儘速完成資安專職人員配置及專業證照、職能評量證書的要求，除於資安推動小組會議研議及追蹤外，並可評估將資通系統及資源向上集中，由上級機關統籌辦理，集中資安作業相關資源。

三、108年資通安全事件通報情形

資安事件通報依據與目的

□依據

– 資通安全管理法第14條、第18條及資通安全事件通報及應變辦法

□目的

– 為即時掌控資通安全事件，並有效降低其所造成之損害，公務機關應建立資通安全事件之通報及應變機制。

– 考量公務機關於知悉資通安全事件後，應進行調查、處理及改善工作， 公務機關應向上級機關提出資通安全事件調查、處理及改善報告，並送交行政院，以利上級機關監督，並得據以提供必要之協助。

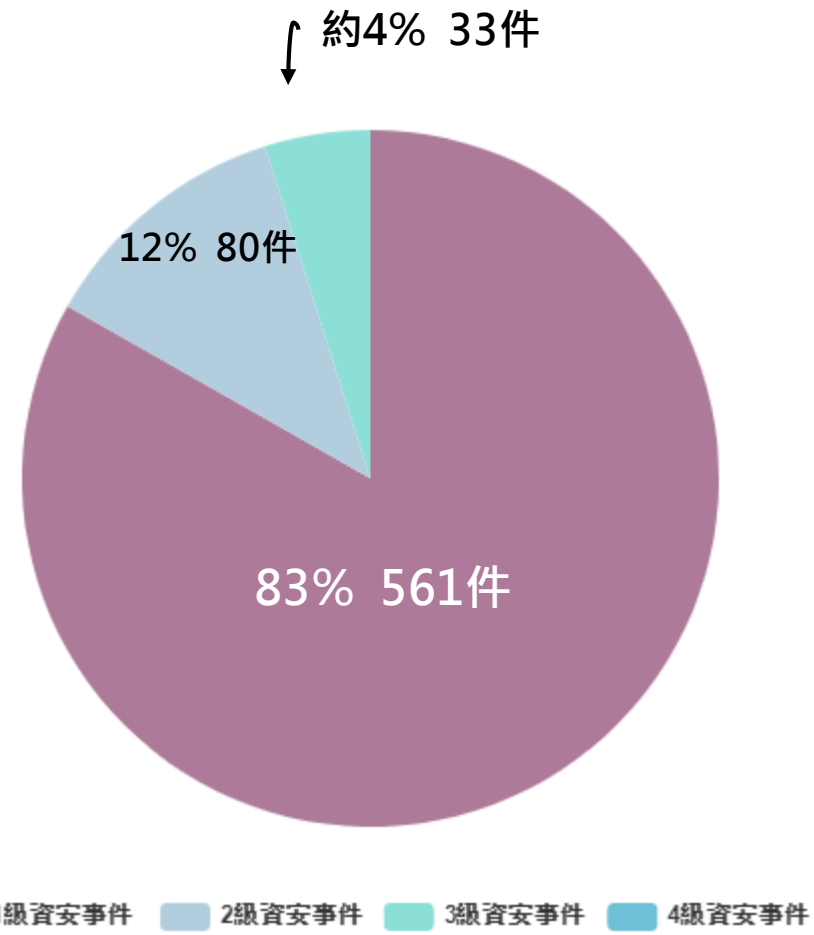
資通安全事件通報及應變辦法

- 機關應依資通安全事件通報及應變辦法之各階段作業時效確實辦理資安事件通報。
- 公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。

	事件通報	完成審核(上級或監督機關)	完成事件損害控制或復原作業	提交事件調查、處理及改善報告
起算時間點	知悉資通安全事件後	接獲事件通報後	知悉資通安全事件後	完成損害控制或復原作業後
1、2級資安事件	1小時	8小時	72小時	1個月內
3、4級資安事件		2小時	36小時	

108年資安事件通報執行情形

- 108年共接獲674件資安事件通報，其中76.11%(513件)為各機關接獲技服中心警訊通告後所進行之通報。
- 通報案件包含
  - 一級資安事件561件
  - 二級資安事件80件
  - 三級資安事件33件
    (包含21件實兵演練通報)



108年資安事件通報時效

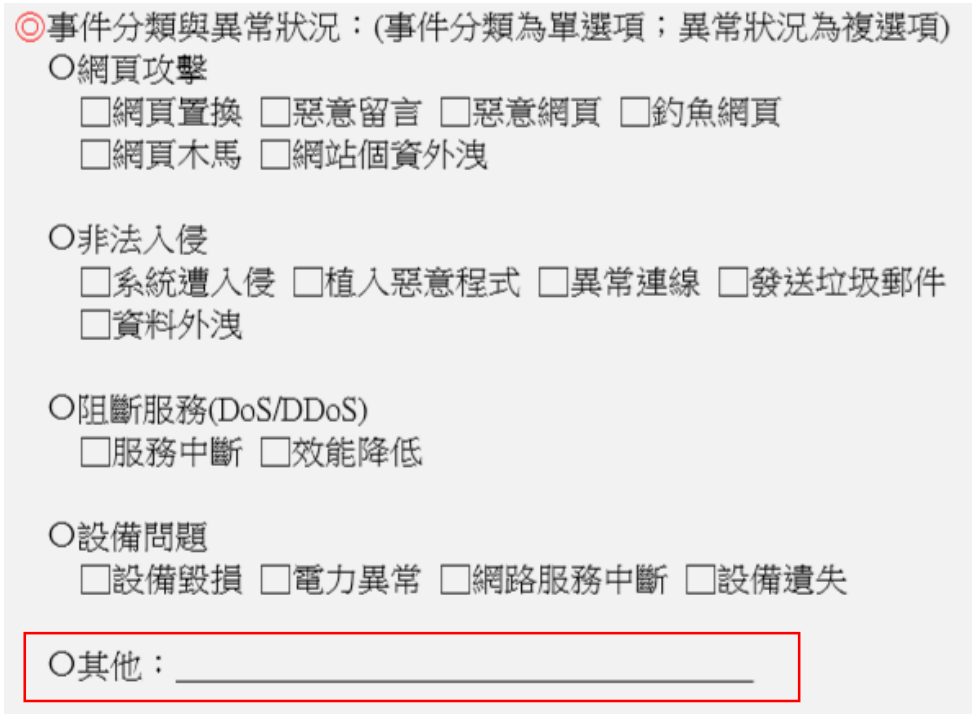
- 通報階段，機關逾時比率約43%，常見原因：
  - 不熟悉資安事件通報流程
  - 誤認為無需通報
  - 機關以資安事件數量作為KPI
- 後續重點
  - 加強宣導應依規定時限通報，建議可以資安事件的通報、應變處置到最後的結報的花費時間做為為KPI。
  - 研擬通報逾限相關獎懲建議：請機關說明逾限原因及改善作為，如無合理原因或未改善，應有獎懲建議。

	通報		應變處置		結報		審核		總通報數
	逾時	未逾時	逾時	未逾時	逾時	未逾時	逾時	未逾時	
數量(件)	290	384	179	495	22	652	13	661	674
比率	43.03%	56.97%	26.56%	73.44%	3.26%	96.74%	1.93%	98.07%	
平均逾時時間	2天21時58分		10天11時54分		50天10時12分		29天8時13分		

註１：逾時時間計算已扣除１小時的通報時間
註２：平均逾限係以384件逾限時間計算

資通安全事件通報常見問題(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。



◎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：_____

資通安全事件通報常見問題(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訊系統、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】

四、108年網路攻防演練辦理情形

網路攻防演練依據與目的

◘依據

– 資通安全事件通報及應變辦法第18條、第19條

◘目的

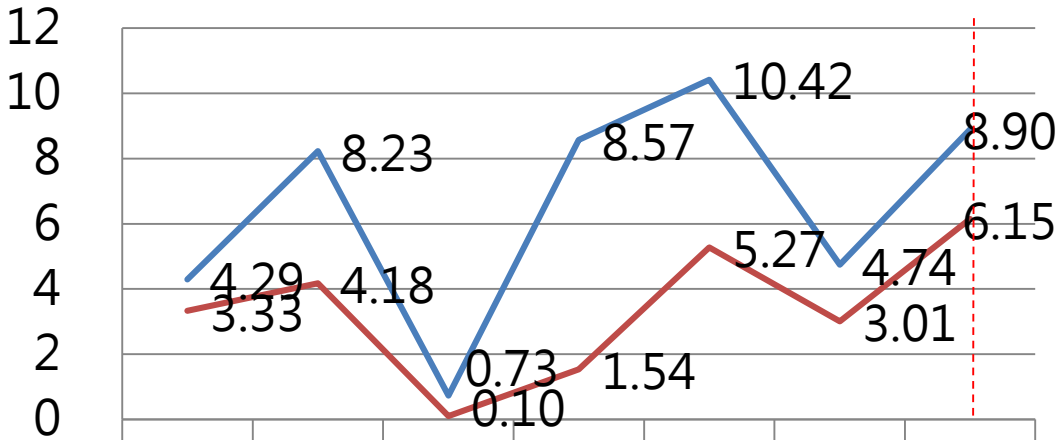
– 強化政府機關與所轄面對資通系統在資安事件發生時之緊急應變、系統復原及協調管控等能力。

– 檢討我國整體資安防護措施，並研討資安防護精進作為。

108年網路攻防演練內容介紹

102至108年郵件社交工程演練結果

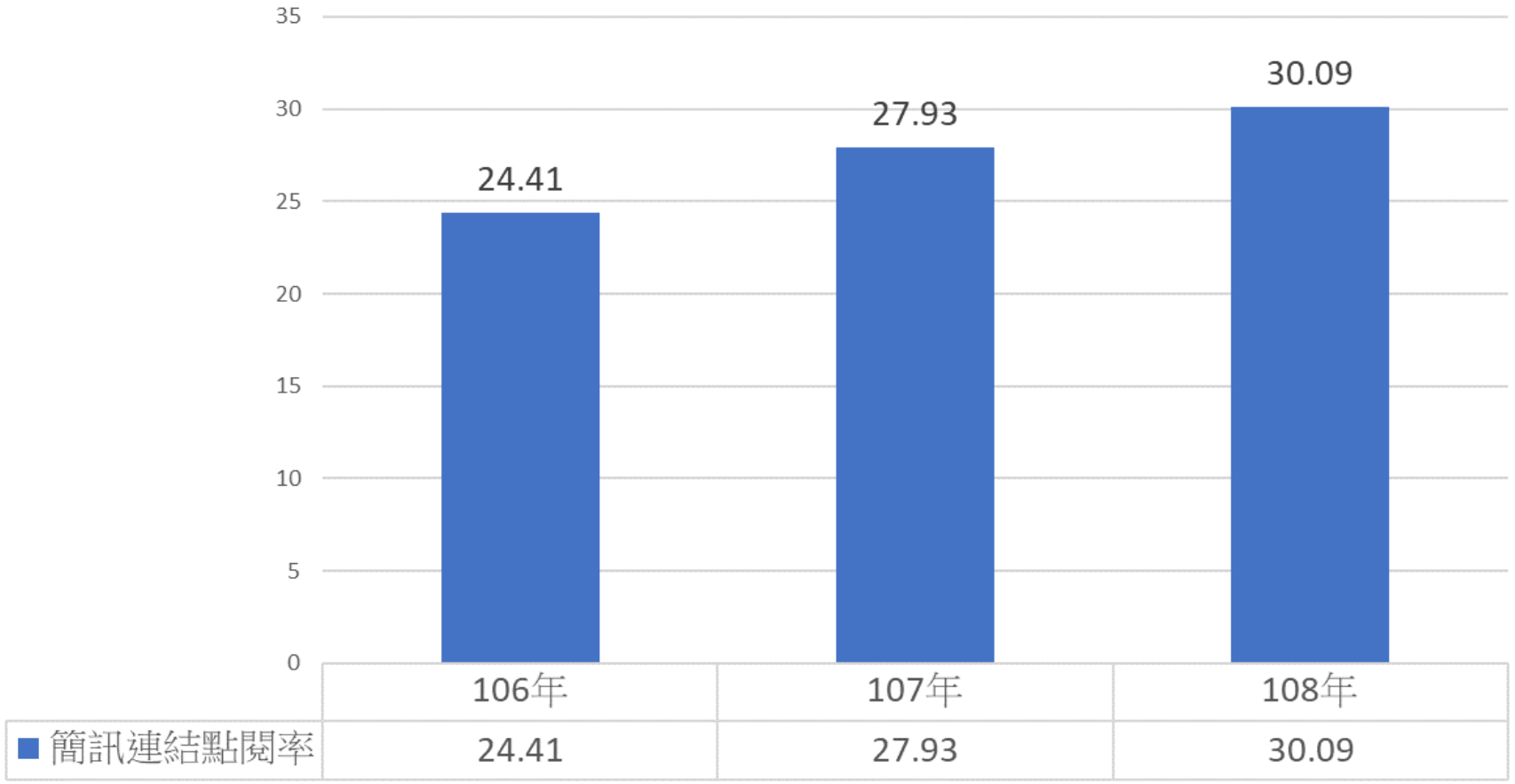
- 近期惡意電子郵件攻擊所用議題越趨精準，為避免因瀏覽惡意電郵，影響網路安全、或致重要資訊外洩。有效提升公務人員對電子郵件的警覺性，108年提升演練郵件的擬真程度，並增加及優化點閱率較高類別：**公文類及財經類**，如會議記錄、收據、對帳單等，故郵件開啟率為歷年次高，郵件附件/連結點閱率為歷年最高



	102年	103年	104年	105年	106年	107年	108年
郵件開啟率(%)	4.29	8.23	0.73	8.57	10.42	4.74	8.90
郵件點閱率(%)	3.33	4.18	0.10	1.54	5.27	3.01	6.15

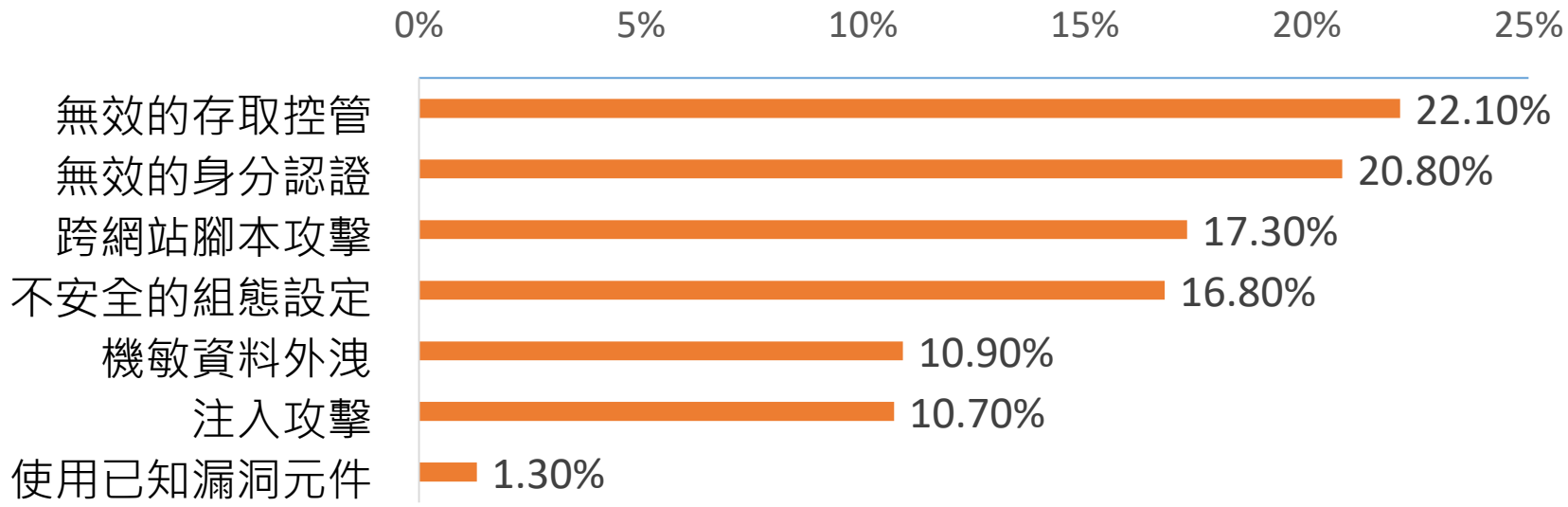
106至108年簡訊社交工程演練結果

- 106年首次執行簡訊社交工程演練
- 108年簡訊連結點閱率為歷年最高



108年資通系統實兵演練

- 與各機關確認其對外系統做為受測範圍，共針對4,264個系統實際攻擊。
- 如被攻擊成功，演練機關應依限完成通報應變，並完成弱點修補。108年計有以下7種類型之弱點。
- 可到技服中心官網參考108第2次政府資通安全防護巡迴研討會的簡報，有108年實兵演練發現的弱點詳細介紹。



108年資通系統實兵演練-弱點及改善建議(1/3)

◘無效的存取控管(22.1%)：

- ➢如不須登入即可直接操作使用者帳號、一般使用者可越權使用管理者的功能。

◘改善建議：檢視每個網站頁面是否落實權限控管

- ➢部分系統使用相同網頁程式，導致攻擊者可在極短時間內取得多個系統之設計資料。
- ➢或以轉導網頁機制之缺陷，攻擊者修改回應封包標頭之方式繞過身分驗證機制，進而執行頁面功能。
- ➢建議針對相同模組之資通系統應加強管控，並逐一頁面落實權限控管，避免攻擊者從中跳脫。

108年資通系統實兵演練-弱點及改善建議(2/3)

◘無效的身分認證(20.8%)：

利用程式中的身分驗證缺陷(網站設計不良、密碼太簡單、忘記登出) 取得更高權限(盜用帳號/身分)進行攻擊行為。

◘改善建議：強化通行碼管理機制

- ➢部分機關允許使用與電子郵件帳號相同之通行碼，一旦電子郵件帳號遭取得，透過已破解之通行碼進而獲得業務之機敏資料或系統管理者權限。
- ➢因此，建議應全面強化通行碼管理機制，並檢測所有系統之通行碼皆遵循通行碼管理機制，避免相同通行碼之組合。

108年資通系統實兵演練-弱點及改善建議(3/3)

◘跨網站腳本攻擊(17.3%)：

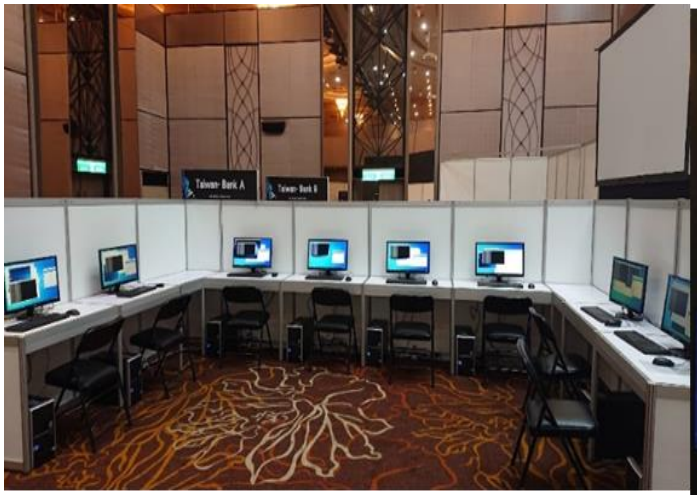
利用程式碼將惡意網站嵌入至正常網頁中，欺騙使用者進行存取，以擷取使用者私密內容；在網頁插入攻擊語法，當使用者或管理者讀取到具有問題的網頁時，就會受到攻擊。

◘改善建議：過濾使用者輸入資料

- 建議使用白名單的方式，針對每個欄位都明確定義出它該有的形式。
- 建議在伺服器端網頁程式對所有參數進行過濾或取代，避免使用者輸入任何網頁語法及程式碼，例如：僅能輸入0至9之字元或過濾與取代「> <)(" ' % ; # & + - 」符號。

跨國攻防演練(CODE 2019)

- 跨國網路攻防演練（Cyber Offensive and Defensive Exercise，CODE 2019），以金融資安環境為主軸，本次演練有別於過去以情境演練方式，108年首次改採實兵演練方式辦理，使用財團法人國家實驗研究院國家高速網路與計算中心所建置之模擬環境邀請國內外政府資安攻擊好手，與我方金融機構組成之防守聯隊共同進行實戰演練，提升彼此資安專業技術與應變能力。



五、108年資通安全稽核執行成果

資通安全稽核依據與目的

◘依據

- ➢資通安全管理法第7條、第13條及特定非公務機關資通安全維護計畫稽核辦法

◘目的

- ➢依資通安全管理法規定，檢視機關資通安全防護作為之落實情形
- ➢透由資安稽核制度，協助政府機關強化資安作業之完整性及有效性，確實提升機關資安防護水準

108年稽核作業說明(1/3)

□受稽對象遴選方式

- 自83個候選公務機關及特定非公務機關中，遴選10個公務機關及5個特定非公務機關執行稽核作業

□稽核小組組成

- 由稽核領隊、稽核委員(7位)、技術檢測人員、工作人員組成，共同執行資安稽核作業，另安排觀察員(1-2位)。

108年稽核作業說明(2/3)

□稽核進行做法：分2階段進行

- 第1階段為技術檢測(3個工作日)，主要係針對受稽核機關之核心資通系統及使用者電腦進行弱點檢測(共7大檢測項目)。
  1.網路惡意活動檢視
  2.核心資通系統安全檢測
  3.網路架構檢測
  4.網域主機安全防護檢測
  5.物聯網設備檢測
  7.組態設定安全檢測

- 第2階段為實地稽核(1個工作日)，由稽核小組至受稽機關進行實地訪視及審查。

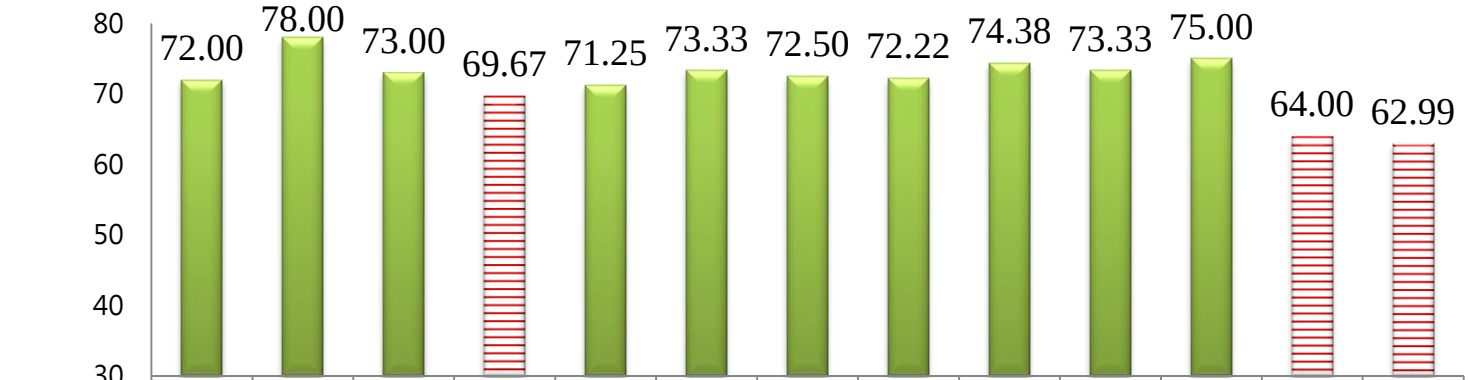
108年稽核作業說明(3/3)

- 稽核作業完成後，將技術檢測執行結果報告、實地稽核報告及共同發現事項等3項資料函送受稽機關與其主管機關，並納入管考追蹤。

- 後續由各受稽機關說明後續矯正措施與改善事項辦理情形，至行政院資通安全會報資通安全作業管考系統(https://spm.nat.gov.tw/)，填寫建議事項辦理情形、進度規劃、佐證資料及自評(完成/持續改善/其他)，再由上級(主管)機關進行第1階段之審核作業，經上級(主管)機關同意後，行政院資安處進行覆核作業。

108年稽核-公務機關整體表現

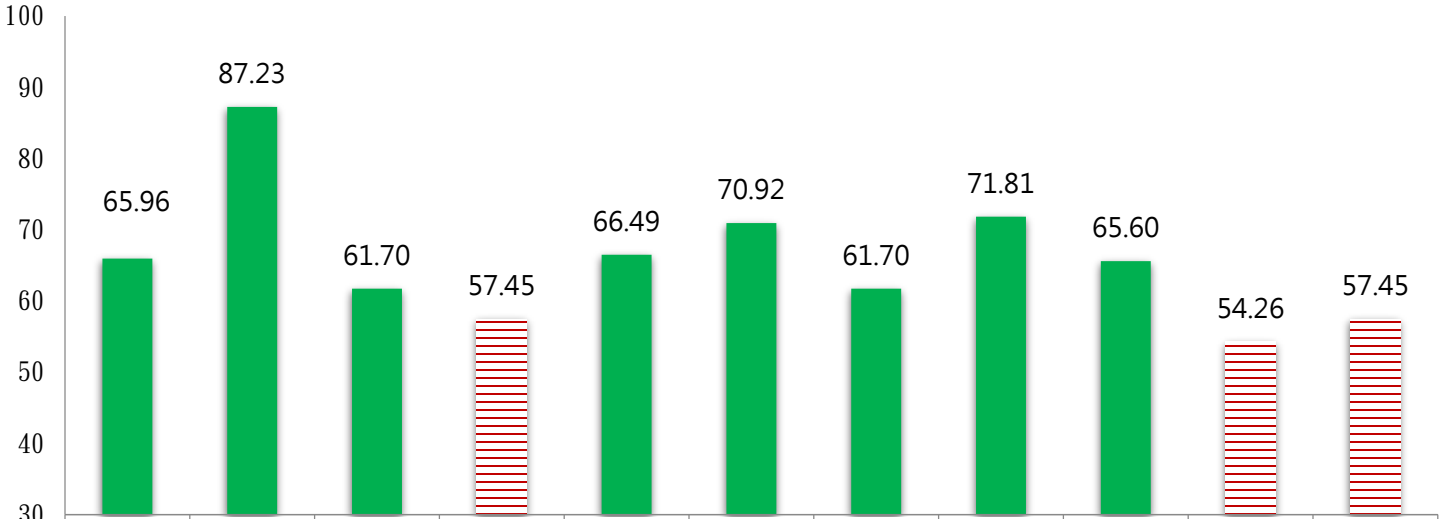
- 「機關首長對資安業務之支持度」表現較好
- 技術檢測成績低於實地稽核整體表現，顯示機關雖有管理制度，惟落實度仍需加強
- 實地稽核中，「資通系統開發及維護安全」表現較不好，顯示機關資訊系統開發之資安管理措施仍待提升



	1.導入資訊安全管理系統範圍之適切性	2.機關首長對資安業務之支持度	3.資源投入資安業務情形	4.資安業務運作規劃及落實	5.資產管理及風險管理	6.人力資源管理	7.資訊委外安全管理	8.所屬機關監督管理	9.電子資料保護	10.通訊與作業安全	11.資安事件通報及處理	12.資訊系統開發及維護安全	技術檢測
平均分數	72.00	78.00	73.00	69.67	71.25	73.33	72.50	72.22	74.38	73.33	75.00	64.00	62.99

108年稽核-特定非公務機關整體表現

- 「機關首長對資安業務之支持度」表現良好
- 「資安業務運作規劃及落實」、「資安事件通報及處理」及「資通系統開發及維護安全」等3項表現較不理想，顯示相關資安管理措施仍待依法規劃並落實



	1.導入資訊安全管理系統範圍之適切性	2.機關首長對資安業務之支持度	3.資源投入資安業務狀況	4.資安業務運作規劃及落實	5.資產管理與風險管理	6.人力資源管理	7.資訊委外安全管理	8.電子資料保護	9.通訊及作業安全	10.資安事件通報及處理	11.資訊系統開發及維護安全
平均分數	65.96	87.23	61.70	57.45	66.49	70.92	61.70	71.81	65.60	54.26	57.45

註：特定非公務機關不進行技術檢測

108年稽核共同發現事項

□策略面

- 機關之核心業務與核心資通系統未能有效界定(資安法施行細則第七條)
- 資安維護計畫與內部ISMS規範文件不一致，且未納入資安法要求(資安法施行細則第六條)
- 特定非公務機關之資安執行小組(資訊單位)，組織層級偏低，未能有效推動資安工作(資安法施行細則第六條)

□管理面

- 機關承辦人員與委外廠商對於資安相關法規認知仍顯不足(應辦事項)
- 資訊委外作業未依法規劃與落實，如防護基準納入RFP、安全檢測、通報程序、稽核等(資安法施行細則第四條)
- 對於所屬機關之稽核規劃與執行成效尚待加強(如受稽機關遴選原則、檢核表未依機關資安責任等級需求進行規劃等) (資安法第十三、十六、十七條)

□ 技術面(含技術檢測)

- 網路架構安全性仍顯不足，如網段區隔、存取控制未確實等(資通系統防護基準)
- 資通系統安全開發程序未依法規劃與落實(資通系統防護基準)
- 安全性檢測與資安健診之落實尚待加強，且改善追蹤未確實(資通系統防護基準)
- GCB導入之例外管理略顯鬆散，且無追蹤改善機制(資通系統防護基準)
- 物聯網設備資安防護不足(資安法施行細則第六條)

108年輔導第二方稽核

- 為落實資安分層管理監督之精神，擇2個機關示範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2位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：
  1. 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。
  2. 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。
  3. 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。

108年輔導第二方稽核共同發現

- 受稽機關遴選數量稍嫌不足，宜規劃整體稽核計畫
- 宜預先衡量受稽機關之性質、規模、人員數，以決定所須投入查核人力，達稽核成效
- 稽核委員僅對自身熟悉之領域深度訪談，致其他檢核項目未能涵蓋，查核事項受限，且抽樣比例稍微不足
- 稽核委員應了解稽核項目所涉及之稽核準則要求，如資安法規等，以明確查核落實情形
- 稽核報告項目宜明確列入稽核目標、稽核範圍、稽核機關、稽核團隊、受稽核機關介紹、稽核日期與地點、稽核準則之聲明、稽核結論等項目

108年稽核結果改善情形

◘截至109年1月31日各受稽機關之改善進度

類別	技術檢測發現		實地稽核建議事項	
機關回覆狀態	已完成	持續追蹤	已完成	持續追蹤
改善情形數量	90	30	61	107
總計(百分比)	75%	25%	36%	64%

◘尚未全數完成事項之原因

- ➢需爭取經費投入
- ➢已規劃處理，並納入未來採購
- ➢需時間調整內部管理制度
- ➢屬中長期規劃，需分年、分階段落實

六、總結

精進建議

- 上級機關應視所屬機關之維護計畫實施情形予以輔導、協助
- 上級機關應稽核其所屬機關的資安維護計畫實施情形

- 機關應確實依規定於期限內辦理資安事件通報
- 資安係風險管控，勿以資安事件數量作為KPI，可改以資安事件的通報、處理、結報的花費時間

- 強化機關同仁對資安法的了解與熟悉，確實辦理資安作業
- 加強對所屬機關稽核機制規劃、執行與追蹤改善

- 應落實辦理資安防護作業，並確實追蹤改善
- 注意系統使用者權限控管、強化通行碼管理機制、防止跨網站腳本攻擊

其他注意事項

- 勿使用具資安疑慮之產品
- 勿使用公務帳號註冊外部服務
- ISMS的「導入」與「驗證」請分開採購
- 資安會報(https://nicst.ey.gov.tw) -資安法專區
  - 資安法常見問題
  - 資通安全專業證照
  - 資通安全管理法中英文版
- 109年規劃辦理資通安全管理法檢討，後續將函請機關提供法規調整及執行建議。

結語

- 各上級、監督或中央目的事業主管機關
  - 掌握所屬、所管(特定非)公務機關之資通安全維護計畫實施情形，進行必要性之指導或協助，並辦理稽核作業
- 各納管對象
  - 機關資通安全維護計畫範圍應涵蓋全機關，確實盤點並識別核心資通系統，建議邀集機關跨單位共同擬定，並共同落實維護計畫內各相關工作

報告完畢
敬請指教