111年資通安全管理法
近期推動及宣導事項

數位發展部資通安全署

111年7月

大綱

一. 資安防護建議及近期事件案例分享

(一)資通安全稽核

(二)資安攻防演練

(三)資安事件通報

二. 資安法常見議題

(一)第三方安全性檢測及元件盤點

(二)因應疫情之資安時數認列調整

(三)VANS導入發現問題宣導

三. 重要政策宣導

(一)具敏感性或國安(含資安)疑慮之業務範疇

(二)資通系統籌獲各階段資安強化措施

(三)資通安全管理法驗證方案特定要求

(四)防疫資訊及系統管理

四. 參考資訊

一、資安防護建議及近期事件案例分享

(一)資通安全稽核

(二)資安攻防演練

(三)資安事件通報

資安防護建議

- 就主管機關資安相關作業發現，提出資安防護建議及應辦理事項，供機關參考依循

一、資安防護建議及近期事件案例分享

(一)資通安全稽核

(二)資安攻防演練

(三)資安事件通報

資通安全稽核

- **稽核準則**
  - 資通安全管理法及其子法、國家資通安全發展方案、受稽機關之資通安全維護計畫、CNS 27001:2014(ISO 27001:2013)、ISO 20000-1:2018
- **稽核小組**
  - 領隊1人、稽核委員7人(策略面2人、管理面2人、技術面3人)
- **稽核範圍**
  - 受稽機關資通安全維護計畫所含之全機關及核心資通系統各項資通安全管理政策、程序等
- **稽核方式**

稽核分組	資安等級A級公務機關	資安等級B級公務機關	特定非公務機關
數量	5	6	5
技術檢測	√		
實地稽核	√	√	√

資安稽核發現-策略面

策略面-共同發現事項

- 未落實核心業務及核心系統之界定，且資通安全維護計畫及實施情形填報內容有所差異
- 資通安全目標設定未盡妥適，將資安事件發生次數納為量測指標

核心業務：由各機關依其組織法規自行界定，須注意非資訊相關業務亦須界定

核心系統：

1.**支持核心業務持續運作必要**之系統

2.**防護需求**等級為**高**之系統

應檢視機關資通系統，整體規劃整併，避免系統過多所致之維運負荷及資安破口

→ 核心業務及核心系統如有變更，除修正維護計畫外，其實施情形亦應確實填報

→ 系統管理單位如有系統變更(新增、調整)事宜，應有相關流程，告知系統盤點彙整單位，避免遺漏

→ 系統彙整單位應定期比對系統盤點資料是否有落差(系統名稱及數量不一致)，適時提報資安長知悉

考量資安目標之妥適性，勿以資安事件發生次數為資安目標，以避免影響通報分享

資安稽核發現-管理面

管理面-共同發現事項

- 資訊資產盤點範圍與內容完整性不足
- 資通服務委外作業未於合約或建議書徵求文件明確規範防護基準需求

1.資訊資產**盤點範圍**須包含機關全部單位，**非僅限資訊單位**，應掌握各單位資料，並**定期比對**盤點資料是否有落差(如系統名稱及整體數量不一致)
2.有關運用計畫經費所籌獲之資通系統亦應納入盤點

1.依資安法施行細則第4條規定，對於委外作業安全應建立相關管理程序，從廠商選擇(技術與能力要求)、服務水平、安全控制措施(含保密、處理人員之管理)及廠商績效監控(稽核)與報告機制等，皆應**明確制訂**於管理程序，並**落實於與廠商之合約規範中**
   - 應遵循「資通系統籌獲各階段資安強化措施」各項規定(行政院院臺護字第1110174630號函)，並可參考其中附件：廠商資安管理作業自我評估表(範例)
2.公告招標時即應說明系統防護需求等級，俾據以納入履約要求

資安稽核發現-技術面

技術面-共同發現事項

依據機關提報資料，大部分機關規劃於**檢測當年度完成**弱點**修補**

- 已進行安全性檢測、滲透測試及資安健檢，惟未落實後續修補
- 針對系統使用之外部元件或軟體未妥善管理

1. 機關應就資安檢測之作業發現，追蹤後續修補、複測作業，確認時程妥適性及作業落實情形
2. 建議訂定相關作業程序進行後續追蹤，並適時提報資安長知悉

1. 應針對資通系統使用之外部元件或軟體，建立系統化管理機制，並納入驗收程序
2. 針對相關元件或軟體之安全性漏洞通告，應落實評估更新

可參考「資通系統防護基準驗證實務參考指引」

可至「技服中心網站/共通規範/參考指引」下載

一、資安防護建議及近期事件案例分享

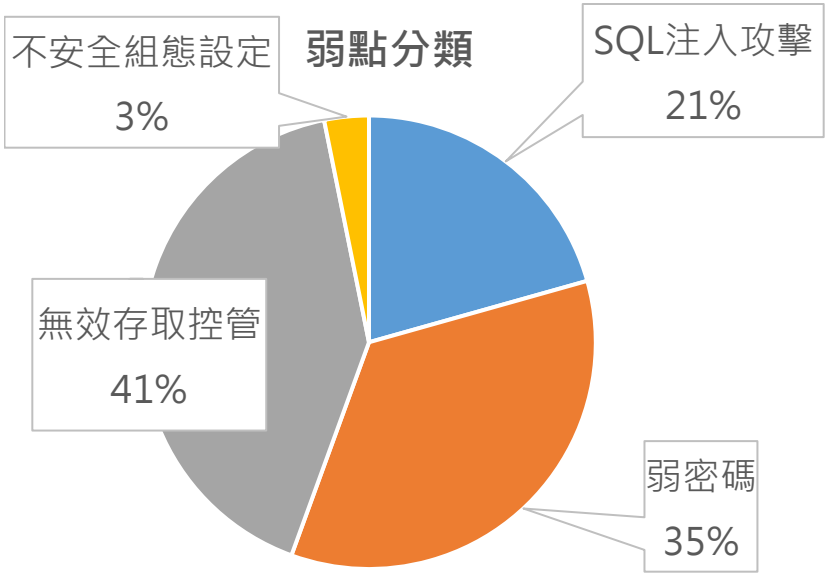
(一)資通安全稽核

(二)資安攻防演練

(三)資安事件通報

資安攻防演練

- 111年網路攻防演練對象，44個A級機關及22個地方政府，共66個
- 資安攻防演練，包含社交工程演練及實兵演練
  - 社交工程演練：已寄發釣魚郵件及簡訊，來誘使機關同仁開啟及點閱，並記錄其上述行為，作為評分依據
  - 實兵演練：就演練對象之對外網站，以不影響機關可用性為原則，進行攻擊
- 從4月18日至6月22日，實兵演練攻擊篇數共有65篇，其中弱點分類如下



攻防演練發現-弱密碼

- 111年(截至6/22)演練機關結果中，弱密碼及無效存取控管之弱點占大多數，比例分別為35%及41%
- 行政院資安處105年11月30日院臺護字第1050185463號函，各政府機關資通系統不應使用身分證字號做為帳號名稱，亦不可使用**弱密碼**做為使用者預設密碼

員工入口網

電子差勤

GCB密碼原則：

1.通行碼長度8碼以上

2.通行碼複雜度應包含英文大寫小寫、特殊符號或數字3種以上

防護建議

- 應強化系統帳號密碼強度及定期更改密碼
- 應加強系統錯誤登入嘗試次數設定及檢視

攻防演練發現-無效存取控管

- 「無效的存取控管」：系統資料存取限制失能，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等問題

防護建議

- **檢視**每個**網站頁面**是否**落實權限控管**
- 如**各頁面**皆使用**相同網頁程式**，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

一、資安防護建議及近期事件案例分享

(一)資通安全稽核

(二)資安攻防演練

(三)資安事件通報

資安事件通報

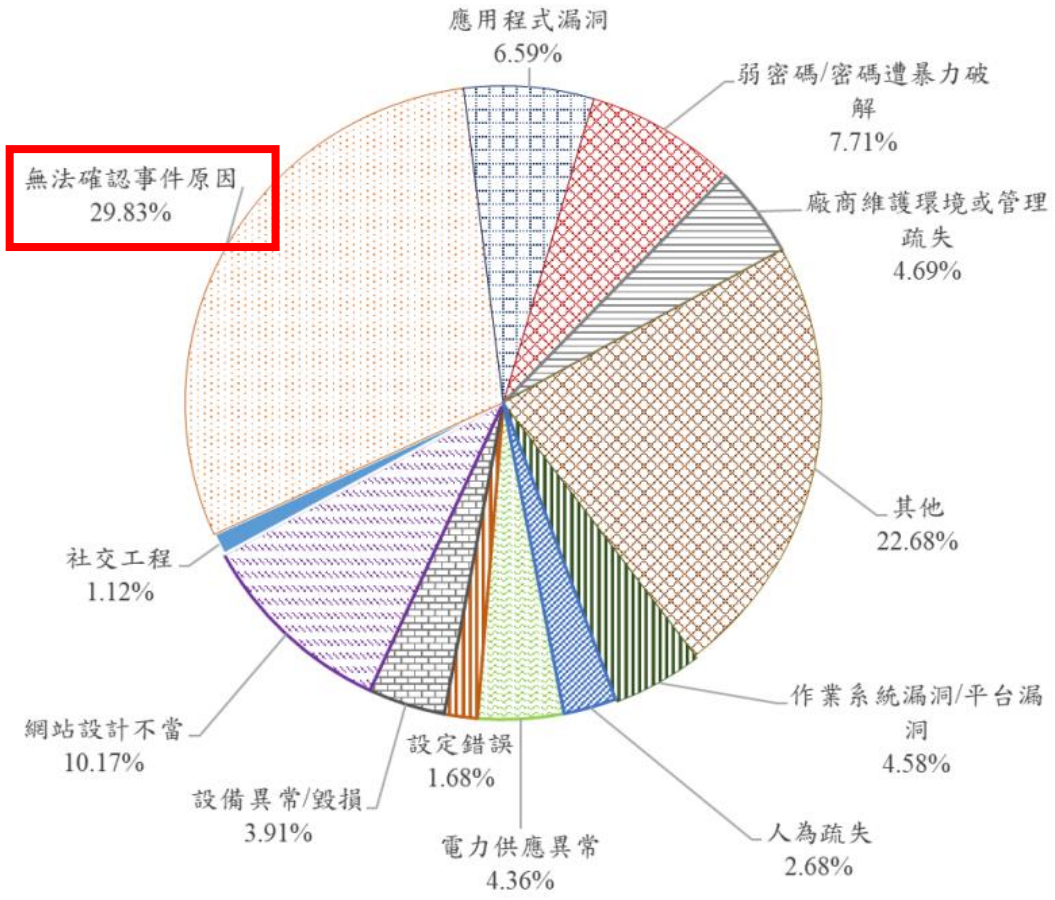
- 110年接獲之資安事件中，有2.37%為3級重大資安事件
- 110年3級事件以個資外洩事件居多，其原因
  1. 網站設計不當
  2. 應用程式漏洞導致資料外洩之外
  3. 使用Google表單蒐集民眾資料，因權限設定不當致使民眾可瀏覽他人填寫之資料

防護建議

- 分級辦法附表十之防護基準所列相關控制措施含
  1. 系統開發階段執行「原始碼掃描」安全檢測
  2. 系統測試階段執行「弱點掃描」及「滲透測試」安全檢測
- 若以Google表單蒐集個人資料等機敏資訊，務必針對權限設定加強控管並妥善設定，避免個資外洩發生

資安事件發生原因

- 110年資安事件發生原因比例如下，「無法確認事件原因」近30%，多因無法確認事件原因僅能採取應變作法



為了解事件根因，據以精進防護，應落實以下控制措施：

1. 保留相關軌跡資料，日誌保留至少六個月
2. 事先規劃留存之系統日誌資訊及容量等條件
3. SOC監控範圍至少包含EDR及「資通安全防護」之內容、AD與核心資通系統之設備紀錄及資通服務或應用程式紀錄

資安事件案例分享(1/2)

事件摘要

- 民眾收到非本人之身分證字號、姓名相關行政處分通知(電子郵件)
- 經機關調查，係該OO系統之帳號申請機制問題，讓使用可直接於網頁申請帳號，未對申請者進行身分審核程序，導致民眾誤申請到業務處理帳號，收到應僅寄送給特定機構之通知(包含他人個資)

應變作法

1. 儘速下架、更正系統功能，並重新確認、測試各項功能之權限控管機制及設定是否確實符合需求
2. 全面清查系統帳號，針對不符規則及久未使用之帳號進行對應處理，如停用或刪除帳號

改善建議

落實資通系統防護基準之帳號管理相關控制措施，如建立帳號審核程序、定期審核帳號資料、定義系統使用情況及條件

資安事件案例分享(2/2)

事件摘要

- 系統於程式模組更新後，誤植權限至全部使用者，導致使用者均具備最高權限
- 經機關調查，有系統使用者不當瀏覽並下載資料及個資

應變作法

1. 儘速下架系統，中斷網路連線
2. 重新設定使用者權限
3. 檢視系統LOG，掌握事件影響範圍

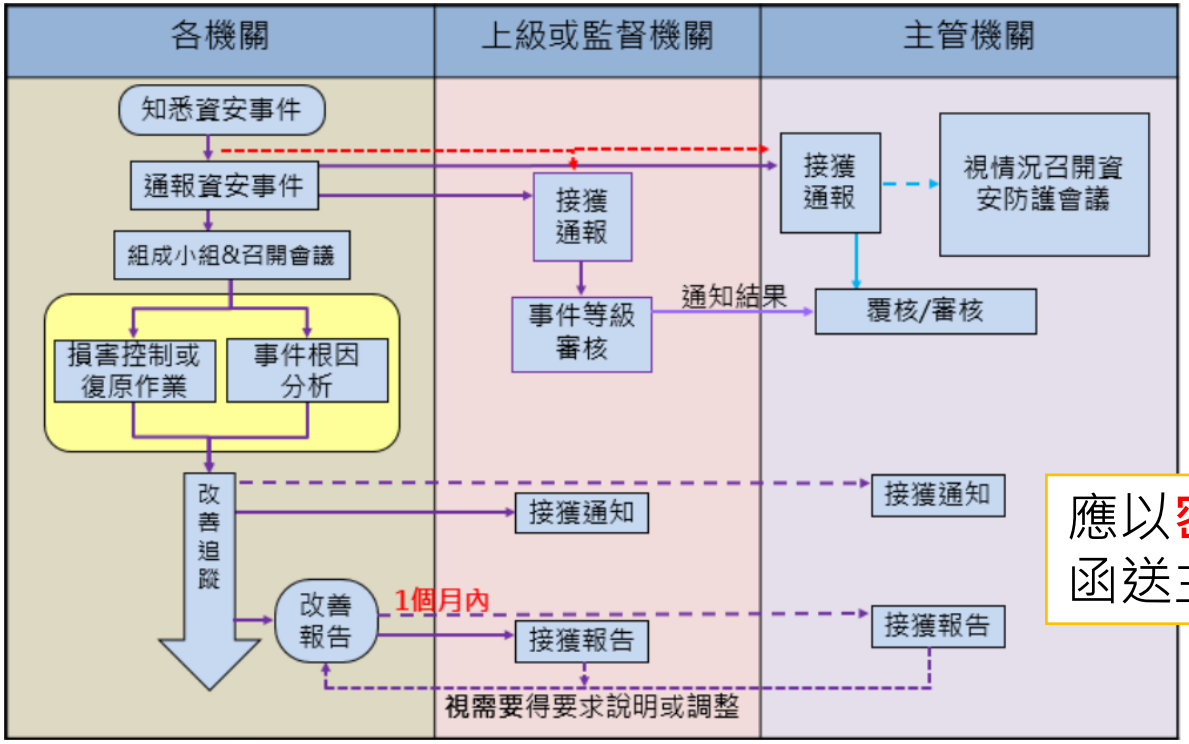
改善建議

1. 機關應訂定系統版本控制程序，於功能更新、調整後，應針對調整處重新測試，完成程序後才能上線
2. 機關於外洩後亦應依個資法規定，查明後以適當方式通知當事人

足以使當事人知悉或可得知悉之方式

通報問題宣導-重大事件函送主管機關

- 依「各機關資通安全事件通報及應變處理作業程序」規定：**第三級或第四級**資通安全事件，於**完成應處後1個月**，應另以**密件公文**將**調查、處理及改善報告**送交**主管機關**及**上級或監督**機關



行政院109年11月9日院臺護字第1090195231號函

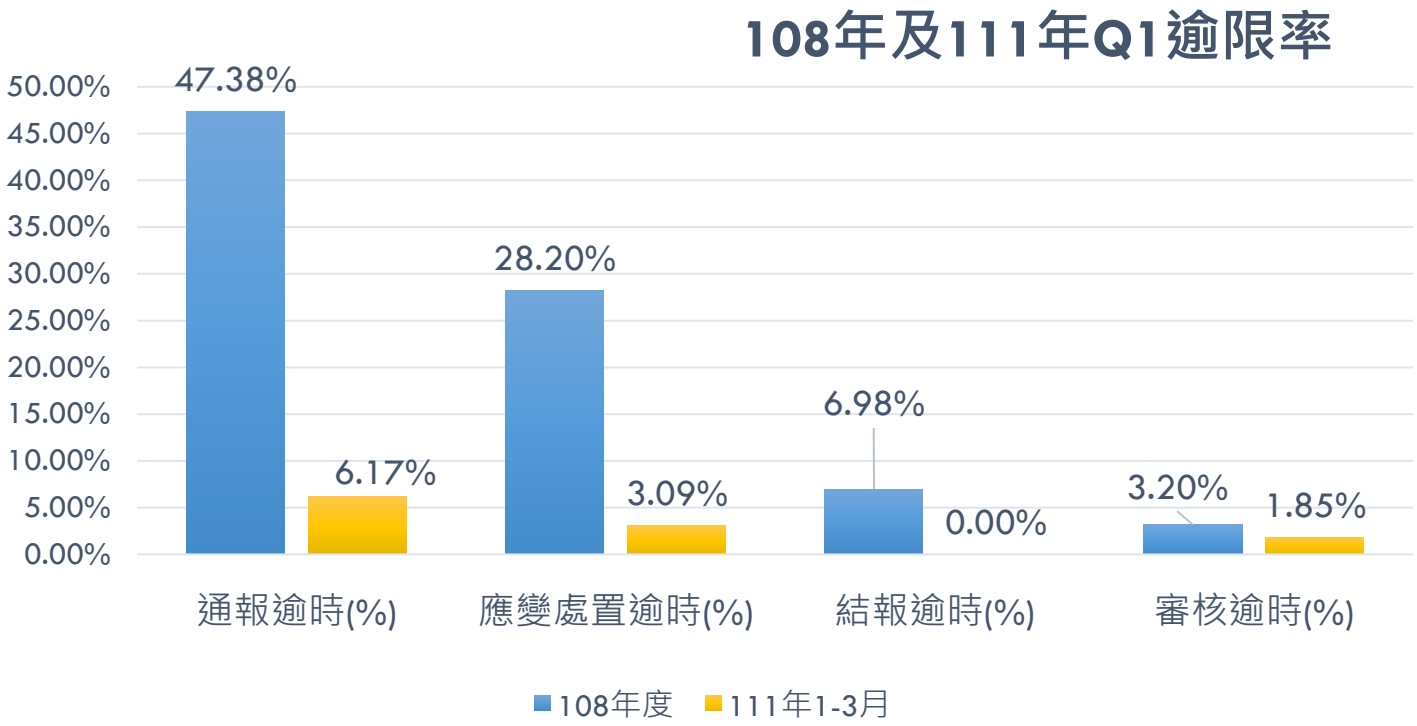
通報問題宣導-演練時通報

- 各機關執行通報及應變演練，請於演練網站做通報

通報應變**演練**網站：https://www.ncert.nat.gov.tw/exer/

通報應變網站：https://www.ncert.nat.gov.tw/

通報問題宣導-通報逾時

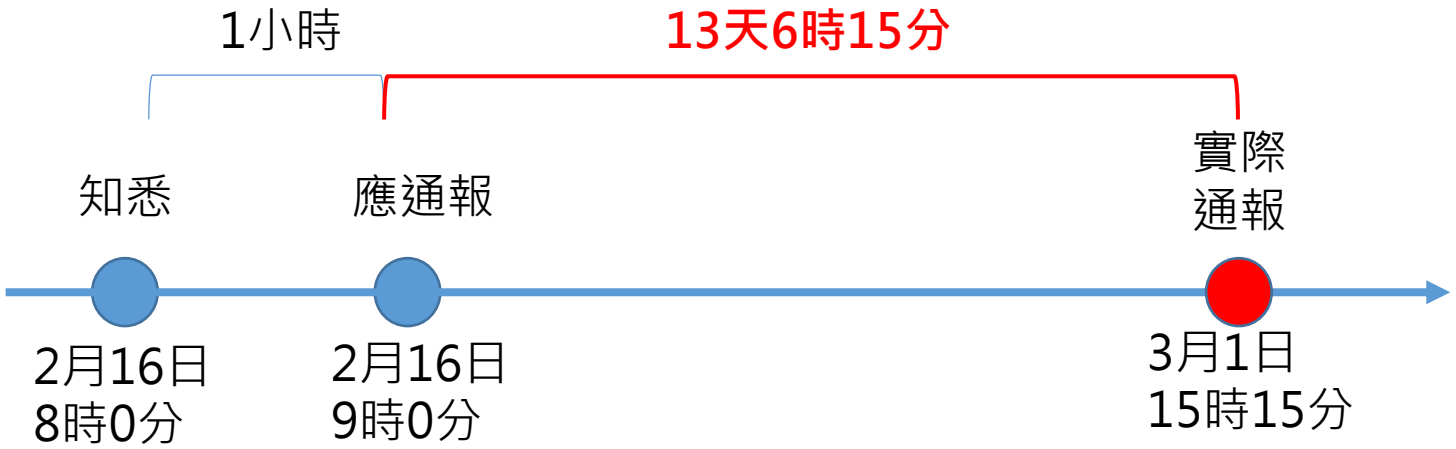


	事件通報	完成審核 (上級或監督機關)	應變處置	結報 (提交調查、處理及改善報告)
起算時間點	知悉事件	接獲通報	知悉事件	完成應變處置
1、2級事件	1小時	8小時	72小時	1個月內
3、4級事件		2小時	36小時	

資安事件通報逾時案例

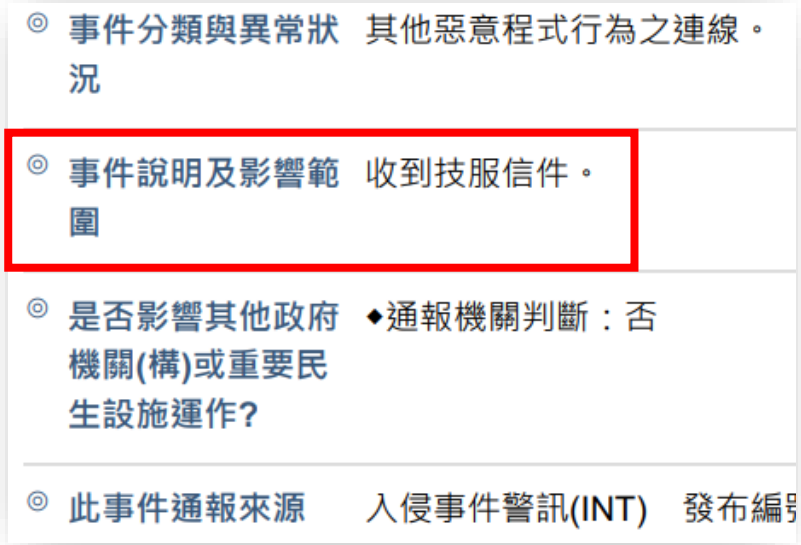
□通報逾時案例　(知悉1小時)

A機關111年**2月16日8時**通知其所屬B機關，A機關所管FB社團遭人張貼販賣老人慰問金個人資料的貼文，B機關雖有向警察機關報案，但卻遲至111年**3月1日15時15分**始通報3級資安事件，逾時**13天6時15分**



通報單事件說明問題-案例分享(1/2)

- 事件通報須提出通報單，其中事件說明及影響範圍應就目前所知部分儘量敘明事件相關資訊，錯誤態樣如下



◎ 事件分類與異常狀況	其他惡意程式行為之連線。
◎ 事件說明及影響範圍	收到技服信件。
◎ 是否影響其他政府機關(構)或重要民生設施運作?	◆通報機關判斷：否
◎ 此事件通報來源	入侵事件警訊(INT)　發布編號

- **看不出**與事件有關的說明，僅說明收到技服通知要去通報
- 考量通報時效，雖難以完整說明真實情況，惟為了有關單位能即時掌握狀況並提供協助，仍應儘量就所知部分詳實敘明，至少須包含**系統名稱**、**具體時間**、事件**確認方式**、緊急**應變方式**之資料

通報單事件說明問題-案例分享(2/2)

- 以下是說明較詳細的事件通報案例
  - 本機關(OOOO系統)於O月O日O時O分接獲系統使用者回報疑似個資可供瀏覽之情況發生，並於半小時後系統管理人員先將系統下線。與系統承辦人了解相關狀況後，調閱相關稽核LOG，含Web、Server、DB Audit、LDAP等資料，發現所有系統使用者皆取得最高權限
  - 本通報單之事件說明內容值得參考，敘明發生問題之**系統名稱**、知悉事件**具體時間**、**緊急**應變**措施**、事件**確認方式**及初步確認**結果**，有關單位可迅速掌握事件概況，即時提供相關(技術、行政、協調)方面協助

二、資安法常見議題

(一)第三方安全性檢測及元件盤點

(二)因應疫情之資安時數認列調整

(三)VANS導入發現問題宣導

二、資安法常見議題

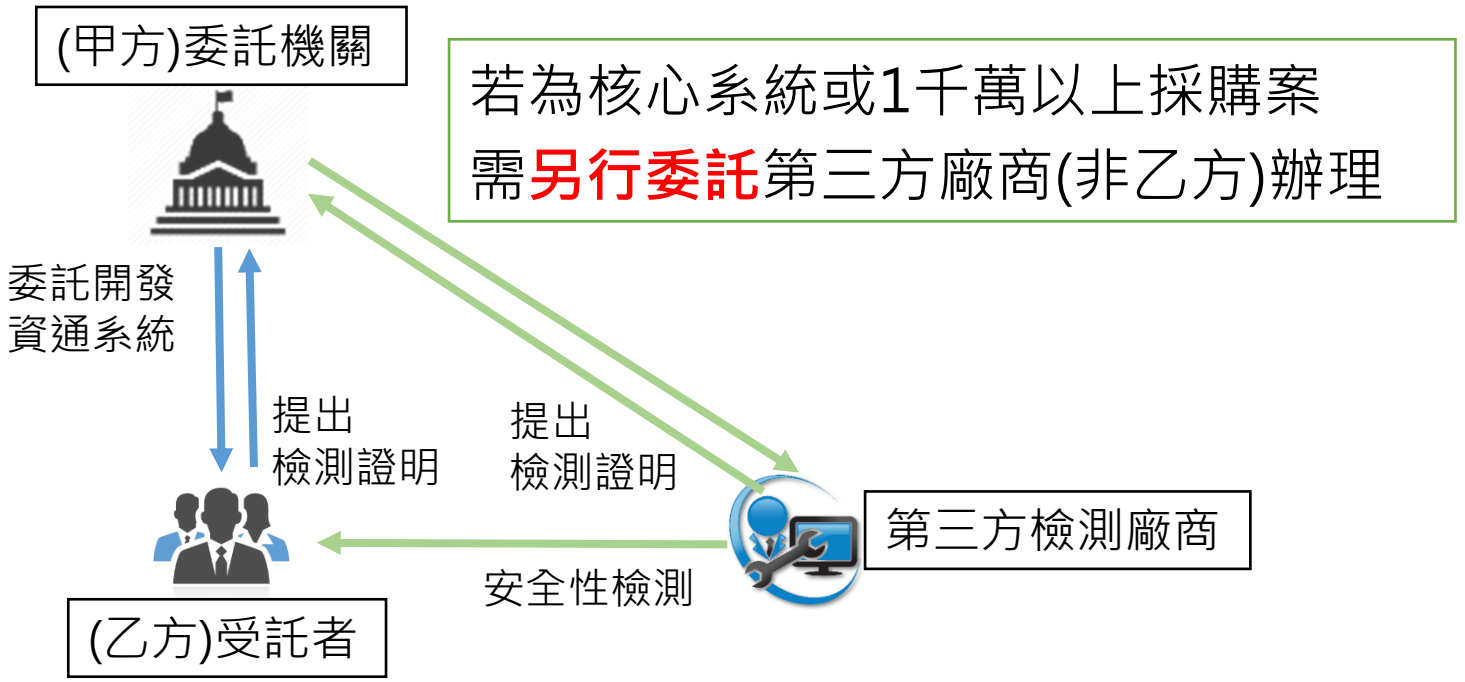
(一)第三方安全性檢測及元件盤點

(二)因應疫情之資安時數認列調整

(三)VANS導入發現問題宣導

第三方安全性檢測及元件盤點

- 資安法施行細則第4條規定客製化資通系統開發，受託者應提供安全性檢測證明，如屬委託機關之核心資通系統，或委託金額達一千萬以上，委託機關應自行或另行委託第三方進行安全性檢測



二、資安法常見議題

(一)第三方安全性檢測及元件盤點

(二)因應疫情之資安時數認列調整

(三)VANS導入發現問題宣導

專業課程訓練及職能訓練時數認定

◘資安法FAQ 3.15

- ➢資通安全專職(責)人員，每人每年需12小時、資通安全專職人員以外之資訊人員每人每2年需3小時之資通安全專業課程訓練或資通安全職能訓練，時數應如何取得？

◘回應

- ➢資通安全職能訓練時數取得方式，係參加經行政院資通安全處認證之資安職能訓練機構辦理之資安職能訓練
- ➢資通安全專業課程訓練可透過以下方式取得：
  - ●技服中心辦理之政府資通安全防護巡迴研討會，或所開設之資通安全策略、管理、技術相關課程
  - ●資通安全專業證照清單上所列之訓練課程
  - ●國內外之公私營訓練機構所開設或受委託辦理之資通安全策略、管理或技術訓練課程

因應疫情相關調整

- 111年5月5日院臺護長字第1110173359號行政院秘書長函

  嚴重特殊傳染性肺炎(COVID-19)疫情第二或第三級警戒期間，相關人員原排定之實體資通安全專業課程訓練及資通安全專業證照課程，得在開課單位與上課學員之合議下，改採遠距上課方式進行，不受資通安全管理法常見問題3.15第三點訓練時數認定上限(6小時)及課程上架至e等公務園、定期更新及提供諮詢機制等限制

- 例子
  - 同仁A參加某短期補習班開設為期二天(12小時)之資安專業課程，該課程因疫情影響改為線上方式辦理，參訓學員仍可取得12小時專業課程時數

二、資安法常見議題

(一)第三方安全性檢測及元件盤點

(二)因應疫情之資安時數認列調整

(三)VANS導入發現問題宣導

應辦事項-政府機關資安弱點通報機制(VANS)

- 截至111年5月24日，**A、B級**機關已有**65%、44%**的機關完成導入，機關應於**111年8月23日前**完成導入，俾符合法遵要求

	111年8月23日前應完成導入				112年8月23日前應完成導入	
	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	公務機關	關鍵基礎設施提供者
已導入機關	42	10	132	9	91	0
尚未導入機關	2	27	84	97	947	54
總計	44	37	216	106	1038	54

- 機關VANS導入情形，已規劃將**納入**資安治理成熟度評估項目

VANS弱點改善措施

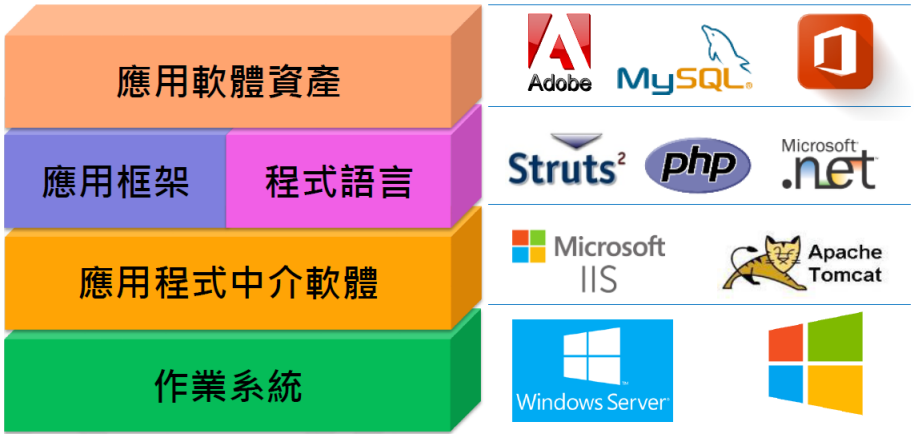
- 當機關發現**高風險**以上之弱點時，應於**1週**內決定**弱點處置方式**並**填寫改善措施**

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

例1：更新處理中，預計XX月完成修補
例2：WSUS定期派送更新 每月定期安裝更新
例3：以使用防火牆、特權帳號管理等措施加強管制

VANS導入發現問題

- 針對部分機關導入VANS情形，**發現問題**及**建議處理方式**如下

序	發現問題	建議處理方式
1	部分機關僅針對**少數單位**之**電腦**進行**導入**，且**未定期上傳**資訊資產	VANS導入範圍應以**全機關**之**資訊資產**為原則，並建議**每月**定期**上傳資訊資產**，另資訊資產**盤點範圍**應包含如下 
2	針對個人電腦及伺服器主機，部分機關僅盤點軟體資產，**未盤點作業系統**	
3	部分機關**僅上傳**有**CPE之資訊資產**，未將無CPE之資訊資產一併上傳	機關應將**全機關**之**資訊資產**(**無論是否有對應CPE**)**上傳至VANS**，以掌握機關整體資產盤點情形

技服中心網站-VANS專區

https://www.nccst.nat.gov.tw/Vans

首頁 > 政府機關資安弱點通報機制(VANS)專區

政府機關資安弱點通報機制(VANS)專區

政府機關資安弱點通報機制(Vulnerability Alert and Notification System, 簡稱VANS)結合資訊資產管理
勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

歡迎透過意見信箱提供您的寶貴意見！

申請作業表單 | 教育訓練教材 | 數位教材影片 | FAQ

帳號申請說明文件
政府機關資安弱點通報系統(VANS
SHA256:32f5624e357317f0af945c

帳號申請表單
附表-政府機關資安弱點通報系統(V
SHA256:a76d6095e5c0ce770b3e3

API介接申請表單
政府機關資安弱點通報系統(VANS
SHA256:9d01bdd812fdabfb7024b2

申請作業表單 | 教育訓練教材 | 數位教材影片 | FAQ

110年政府機關資安弱點通報機制(VANS)實作訓練課程數位教材

政府機關資安弱點通報機制(VANS)實作訓練課程數位教材影片

1-前言與法規政策說明、系統說明、盤點作業v1.0_1110418.zip
【檔案完整性驗證碼SHA256】5bfc3bcad6302dc49d55c2d0fc9c

2-正規化作業v1.0_1110418.zip
【檔案完整性驗證碼SHA256】97d5abc85543dcb8862a441f6c2

3-登錄作業v1.0_1110418.zip
【檔案完整性驗證碼SHA256】62d373a791a8fbfacd98712e168

4-使用自動化工具(盤點、正規化、登錄作業)v1.0_1110418.zip
【檔案完整性驗證碼SHA256】2cf687be697bdeac745f75e6217

5-弱點通知與修補作業v1.0_1110418.zip
【檔案完整性驗證碼SHA256】41e5fd5f55074105b09ae2b55b6

6-更新作業、常見問答v1.0_1110418.zip
【檔案完整性驗證碼SHA256】0387cddc810f7c0eda6187257f82

數位教材影片已依5大導入流程進行區分，供機關參考

三、重要政策宣導

(一)具敏感性或國安(含資安)疑慮之業務範疇

(二)資通系統籌獲各階段資安強化措施

(三)資通安全管理法驗證方案特定要求

(四)防疫資訊及系統管理

三、重要政策宣導

(一)具敏感性或國安(含資安)疑慮之業務範疇

(二)資通系統籌獲各階段資安強化措施

(三)資通安全管理法驗證方案特定要求

(四)防疫資訊及系統管理

涉陸供應方之相關採購情境

採購方	服務供應方	現行處理方式
政府機關	大陸地區廠商	各機關**應**於招標文件**規定**得標及分包廠商**不得**為大陸地區廠商 107年12月30日工程會函釋及109年12月18日本院秘書長函文
	第三地區含陸資成分廠商	1. **適用GPA**之採購，機關**得**依GPA第3條(**安全及一般除外**)規定排除適用 2. **非適用GPA**之採購，**可**於招標文件規定不允許第三地區含陸資成分之廠商參與
	在臺陸資廠商	1. 104年1月27日工程會函釋，辦理資通訊服務採購如屬**具敏感性或國安(含資安)疑慮之業務範疇**，**可**於招標文件中載明不允許陸資資通服務業者參與 2. 經濟部於核准陸資資通服務業投資案時，均**以附加條件等方式**，**限制其從事經公告之具敏感性或國安(含資安)疑慮之業務範疇**

現行適用對象及範圍

- 「具敏感性或國安(含資安)疑慮之業務範疇」已於109年11月上旬更新，經濟部投資審議委員會亦於網站公布相關清單
- 適用範圍

具敏感性或國安(含資安)疑慮之業務範疇

關鍵資訊基礎設施(CII)

影響機關運作或包含個人資料之行政輔助重要系統

主領域	次領域
能源	電力
	石油
	天然氣
水資源	供水
通訊傳播	通訊
	傳播
交通	陸運
	空運
	海運
	氣象

主領域	次領域
能源	電力
	石油
	天然氣
水資源	供水
金融與銀行	銀行
	證券
	金融支付
通訊傳播	通訊
	傳播

主領域	次領域
交通	陸運
	空運
	海運
	氣象
金融與銀行	銀行
	證券
	金融支付

後續辦理事項

- 各政府機關於辦理採購案時，應評估採購標的，如屬於具敏感性或國安(含資安)疑慮之業務範疇，則**可於招標文件中載明不允許在臺陸資資通服務業者參與**

三、重要政策宣導

(一)具敏感性或國安(含資安)疑慮之業務範疇

(二)資通系統籌獲各階段資安強化措施

(三)資通安全管理法驗證方案特定要求

(四)防疫資訊及系統管理

111年5月26日院臺護字第1110174630號行政院函，發布後試行一年

網址：https://nicst.ey.gov.tw/Page/7CBD7E79D558D47C/b280a801-9bad-411f-97a5-54b23b1fe462

資通系統籌獲各階段資安強化措施

- 依據資通安全管理法第9條所定委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形
- 為協助公務機關及特定非公務機關於本法適用範圍內委外辦理相關作業，補充說明委託機關依本法施行細則第4條規定選任或監督受託者之相關行政流程及應注意事項，特訂定本措施

資安強化措施流程圖

委託機關

需求階段

評估系統防護需求等級、資安人力及作業需求

招標階段：標註系統防護需求等級，並於估價單等投標文件中明列資安經費

評選階段：受託者資安作業應納入評選項目，核心資通系統則應包含資安專業評選委員

建置階段

確認開發團隊於系統開發時遵循安全軟體開發生命週期(SSDLC)及重點里程碑

核心資通系統則應聘請外部資安專家為顧問或委員，協助檢視履約程序與成果之相關資安管理作為

核心資通系統且委託金額達一千萬元以上，則應評估導入IV&V

維運階段

確認資通系統維運作業確實依委託機關之資安管理措施落實辦理

受託者應配置適當之資通安全專責人員

得依籌獲案規模及性質，要求受託者就受委託範圍自行辦理稽核作業。

委託機關應定期或不定期對受託者辦理稽核(高)

受託者執行受託業務知悉資安事件(重大)，委託機關應辦理資安稽核，並將稽核結果送交主管機關。

刻調整通報應變網站功能及管考系統功能，若事件發生原因為廠商維護環境或管理疏失，機關應於事件通報之結報單中敘明廠商名稱；並可於管考系統查詢廠商近3年之事件情形(維護環境或管理疏失)，供機關選商參考

資安強化措施常見問題-適用範圍、IV&V

Q：套裝軟體、設備購買、系統維護案，**是否適用**此措施？

A：本措施主要適用於**應用系統開發委外案**，針對「無客製化之套裝軟體」、「網路及資安等資通訊設備購買」、「例行性或不定期之系統維護案」等其他情形，則就可執行項目適用本措施之各項規定

Q：獨立驗證與認證機制(**IV&V**)是指什麼？要做到什麼程度才符合規範要求？

A：IV&V係由**「獨立」第三方執行**，用來檢查一個專案、服務或者是系統**滿足特定規範(驗證)**以及**滿足預期目的(確認)**的過程(如SDLC方法論、技術檢測等)，俾驗證及確認該委託案是否符合規範(資安法、個資法或其他內部規定)並滿足委託機關各項需求(RFP)

資安強化措施常見問題-角色分工

Q：措施所列各作業項目皆應由機關之資安專責(職)人員負責嗎？

A：本措施係強調機關之資安專責(職)人員應參與各式資通系統籌獲案之資安作業，主責單位原則仍為該系統需求或管理單位，資安專責(職)人員係以機關**第二線確認**角色，再次確認受託者是否依委託機關要求辦理各資安作業

應注意事項	系統需求(管理)單位	資安專責人員
SSDLC	監督、確認	(第二線)勾稽確認
專案里程碑及履約資安管理	訂定、監督、確認	

資安強化措施常見問題-資料跨境議題

Q：資料存取、儲存、備份及備援等作業， 其實體設備所在地及資料傳輸是否跨境等相關議題，得要求其**以書面方式揭露**，實務應如何執行？

A：如機關認有需求，得參考本院資通安全會報網站-作業規範-資通系統籌獲各階段資安強化措施之附件-**資料所在地及跨境傳輸切結書(範例)**，要求廠商揭露受託內容涉及大陸廠商及跨境傳輸等資訊

資通系統籌獲各階段資安強化措施

日期：111-06-27　　資料來源：資通安全處

依據資通安全管理法(以下簡稱本法)第九條規定，公務機關或特定非公務機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。為協助公務機關及特定非公務機關於本法適用範圍內委外辦理相關作業，補充說明委託機關依本法施行細則第四條規定選任或監督受託者之相關行政流程及應注意事項，特訂定本措施。

相關檔案

資通系統籌獲各階段資安強化措施 PDF

附件1_廠商估價單_資安作業範例_ ODT

附件2_評選委員評選表_範例_ ODT

附件3_廠商資安管理作業自我評估表_範例_ ODT

附件4_資訊服務採購案之資安檢核事項 PDF

附件5_資料所在地及跨境傳輸切結書_範例_ ODT

網址：
https://nicst.ey.gov.tw/Page/7CBD7E79D558D47C/b280a801-9bad-411f-97a5-54b23b1fe462

三、重要政策宣導

(一)具敏感性或國安(含資安)疑慮之業務範疇

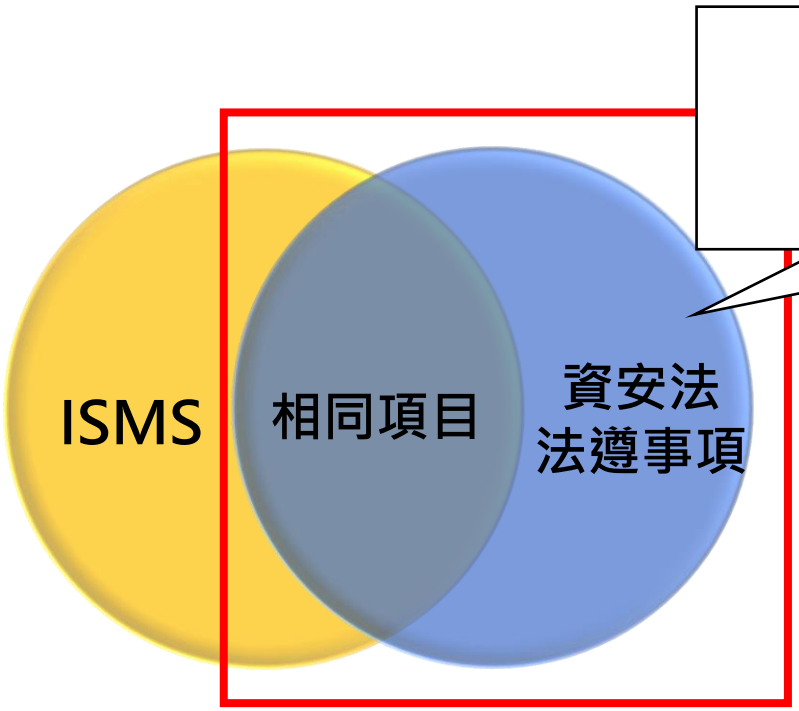
(二)資通系統籌獲各階段資安強化措施

(三)資通安全管理法驗證方案特定要求

(四)防疫資訊及系統管理

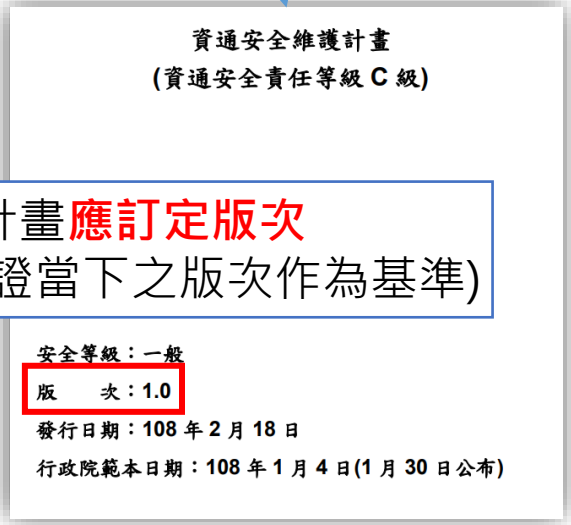
資通安全管理法驗證方案特定要求-目的

- 為加速推動資安法法遵落實，刻正規劃於「資訊安全管理系統認證領域」項下(ISMS)，增加「資通安全管理法驗證方案特定要求」，由公正第三方驗證機構進行驗證



資安法特定要求驗證之驗證範圍
原ISMS驗證項目+資安法規定項目

1.資安維護計畫/實施情形
2.資安責任等級應辦事項
3.資通系統防護基準


資通安全維護計畫
(資通安全責任等級 C 級)

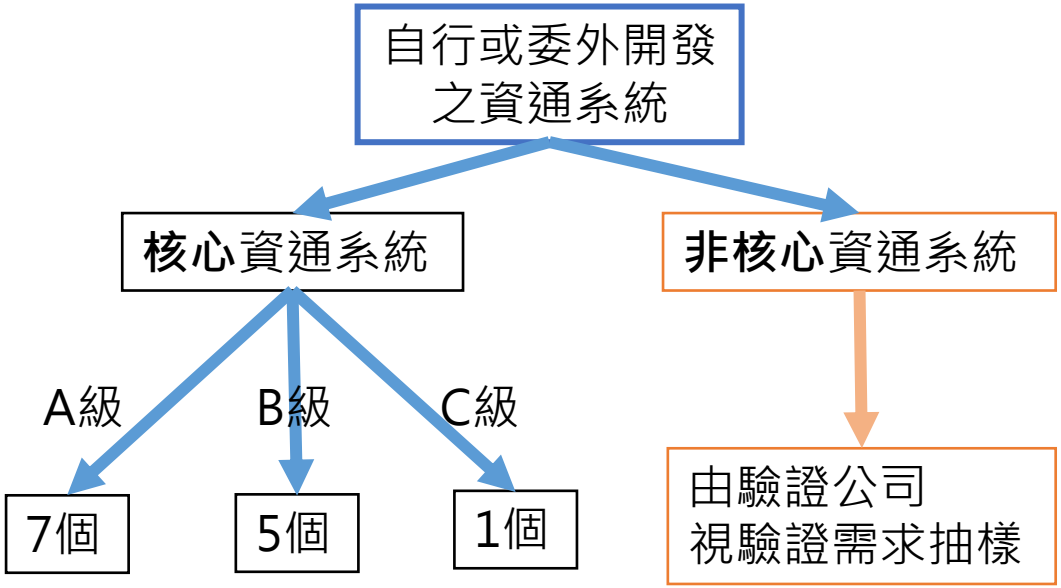
維護計畫**應訂定版次**
(以驗證當下之版次作為基準)

安全等級：一般
版　　次：1.0
發行日期：108 年 2 月 18 日
行政院範本日期：108 年 1 月 4 日(1 月 30 日公布)

核心系統抽樣原則

◘核心資通系統抽樣

- ➢核心資通系統數量基準依機關之資通安全責任等級 A 級、B 級及 C 級分別為 7 個、5 個及 1 個
- ➢核心資通系統數量小於(含)基準者，所有核心資通系統需納入稽核，不允許抽樣；反之則允許抽樣，抽樣原則以未曾接受過查核者為優先



驗證公司之抽樣原則可參考下列因素：
1.資通安全防護需求等級高者
2.屬共用性資通系統者
3.近期執行重大資通系統改版或更新者
4.近2年曾發生資通安全事件者
5.查核結果建議持續關注者

未來規劃

- 請各機關於辦理ISMS驗證時，**納入驗證方案特定要求**
- 未來將**納入資安法**修法

最後更新日期： 2022/04/30 點閱次數： 80

本會自111年5月1日起，開放受理「資通安全管理法驗證方案」之認證服務。

一、行政院資安處制定「資通安全管理法」，以期積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。因應國家推動「資通安全管理法」之政策，落實公務機關與特定非公務機關之法令遵循義務。

二、本會制定「管理系統驗證機構資通安全管理法驗證方案特定要求」，並自111年5月1日起正式開放「資通安全管理法驗證方案」之認證服務。

三、本會認證服務之相關資訊，請參見本會網站https://www.taftw.org.tw/文件專區/認證方案/管理系統驗證機構文件。

三、重要政策宣導

(一)具敏感性或國安(含資安)疑慮之業務範疇

(二)資通系統籌獲各階段資安強化措施

(三)資通安全管理法驗證方案特定要求

(四)防疫資訊及系統管理

111年6月6日指揮中心肺中指字第1114300098號函

防疫所蒐集個人資料管理

- 個人資料蒐集之特定目的消失後，如無保留之必要，**應主動將個人資料予以刪除**
- 機關除防疫相關系統，亦應注意**紙本、個人電腦及雲端空間**儲存之個人資料
- 如有透過**電子郵件**傳遞資料情形，亦應檢視電子郵件之資料留存情形
- 本院已就該等電子資料安全管理機制納入**資通安全稽核**檢核項目內
- 機關建置及維護資通系統，**仍應依資安法相關規定辦理**各項管理措施，如系統盤點、防護需求評估，**符合對應之防護基準措施**；並納入機關整體資安防護，適時稽核確認措施落實情形

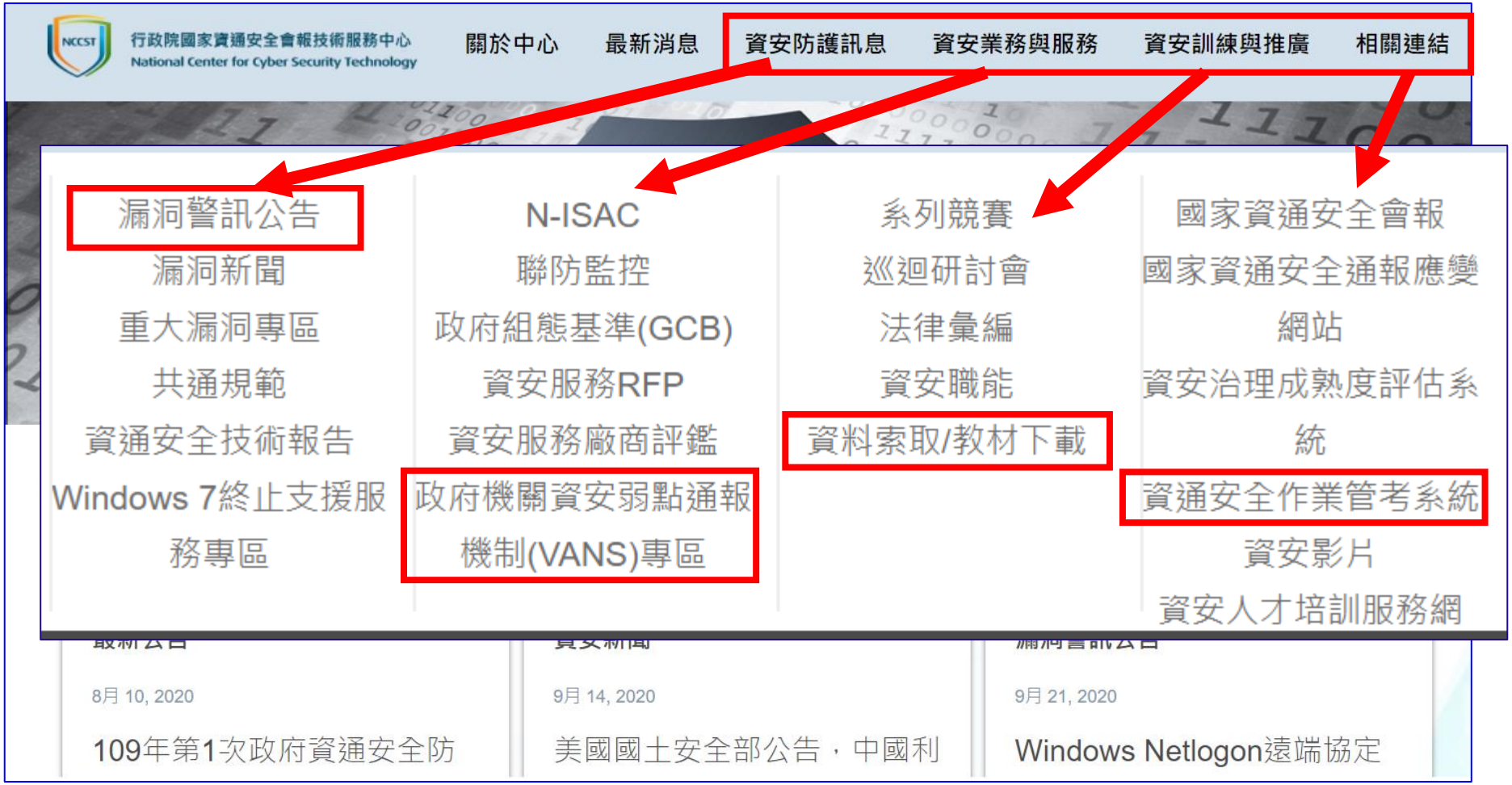
參考資訊

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/



參考資訊-資安管理法採購指引懶人包

- 跨域資安強化產業推動計畫網站(ACW)/產業服務/資安法懶人包 (https://www.acw.org.tw/Match/Default.aspx?subID=38)

1.《資通安全管理法》懶人包

透過流程圖及Step-by-Step大富翁方式快速協助各機關所屬資通安全責任等級與查閱懶人包內容

2.《資通安全管理法》採購指引懶人包

採用管理、技術與認知訓練三構面方式呈現各應辦事項之參考實作方式、參考採購需求項目及相關建議資安服務/產品及廠商

3.《資通安全管理法》採購指引廠商名錄

採用管理、技術與認知訓練三構面方式呈現參考資安服務/產品及廠商名錄

附錄

- 《資通安全管理法》推動參考資安專欄
- 《資通安全管理法》採購指引懶人包諮詢窗口
- 《資通安全管理法》採購指引懶人包相關連結
- 《資通安全管理法》應辦事項實作時程參考

資安是持續精進的風險管理