110年資通安全管理法近期推動及宣導事項

行政院資通安全處

110年11月

大綱

一.110年8月資通安全管理法修法重點
二.109年資通安全維護計畫實施情形
三.資通系統防護基準驗證實務參考指引
四.資安強化措施(委外管理)
五.視訊與即時通訊軟體使用安全注意事項
六.事件應變案例宣導
七.弱密碼議題宣導
八.資通安全管理法驗證方案(草案)
九.參考資訊

110年8月
資通安全管理法修法重點

資通安全管理法修法重點

- 有關資通安全管理法子法修正條文，本院已於中華民國110年8月23日以院臺護字第1100182012號令修正發布施行
- 「資通安全管理法及子法彙整版」最新版已公布於行政院國家資通安全會報網站

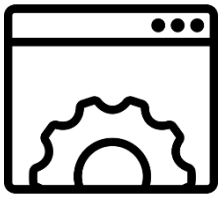
C級機關定義

第六條

各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為C級。

前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。

- 機關有建置維運目錄服務系統、電子郵件系統等具權限區分及管理功能之資通系統，應為C級



自行或委外開發之系統

目錄服務系統

電子郵件系統

- 等級提報調整，比照資安法FAQ 2.11題：機關如有組織變更情形(裁撤、整併、業務調整、新成立、成立籌備處)，其上級機關須於1個月內辦理等級異動作業

應辦事項-VANS及EDR

以附表1-A級公務機關為例

制度面向	辦理項目	辦理內容
技術面	資通安全弱點通報機制	▪ 初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料 ▪ 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料
	端點偵測及應變機制	▪ 初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料 ▪ 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料

項目	資安責任等級	辦理內容
VANS	A、B級公務機關、關鍵基礎設施提供者	一、修正施行後**1年**內　(111.8.23前) 二、初次受核定或等級變更後之**1年**內
	C級公務機關、關鍵基礎設施提供者	一、修正施行後**2年**內　(112.8.23前) 二、初次受核定或等級變更後之**2年**內
EDR	A、B級公務機關	一、修正施行後**2年**內　(112.8.23前) 二、初次受核定或等級變更後之**2年**內

政府機關資安弱點通報(VANS)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

VANS介接說明

資訊資產盤點

逐台運用
批次檔盤點

自行開發程式
盤點

(警政署、台大醫院、苗栗縣稅務局
已開發完成)

使用商用軟體盤點

(目前有14家廠商與技服完成
介接測試，清單詳資通安全
管理法採購指引懶人包)

廠商名稱（以筆劃排序）
ForeScout
中華數位科技股份有限公司
中華龍網股份有限公司
日月晶耀股份有限公司
旭辰資訊股份有限公司
捷睿智能股份有限公司
瑞思資訊股份有限公司
誠雲科技股份有限公司
達煬科技股份有限公司
睿明知通股份有限公司
精品科技股份有限公司
精誠資訊股份有限公司
優倍司股份有限公司
曜祥網技股份有限公司

資訊資產正規化

資訊資產

利用文書處理
軟體轉換CPE

自行開發
程式轉換CPE

利用市面軟體
轉換CPE

使用商用盤點軟體
執行轉換CPE

資產上傳比對

人工至網頁上傳
資產清單

自動定時
以API上傳

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系統)帳號申請說明文件v1.0_1100408.pdf
SHA256:32f5624e357317f0af945cc2fb8a2327a740109f0dbb19d94a67a347b046bb32

帳號申請表單

附表-政府機關資安弱點通報系統(VANS系統)機關管理者帳號申請(異動)單v1.3_1100419.xlsx
SHA256:a76d6095e5c0ce770b3e30c7eef174a088dc66657f89a044e722414eb1fb49b3

API介接申請表單

政府機關資安弱點通報系統(VANS系統)API介接申請(異動)單v1.2_1100419.xlsx
SHA256:9d01bdd812fdabfb7024b2713ec2d417d45ac0c84b43abde58203ba107266e4f

EDR導入說明

□範圍

B級以上公務機關應辦事項：
持續維運及依主管機關指定之方式提交偵測資料

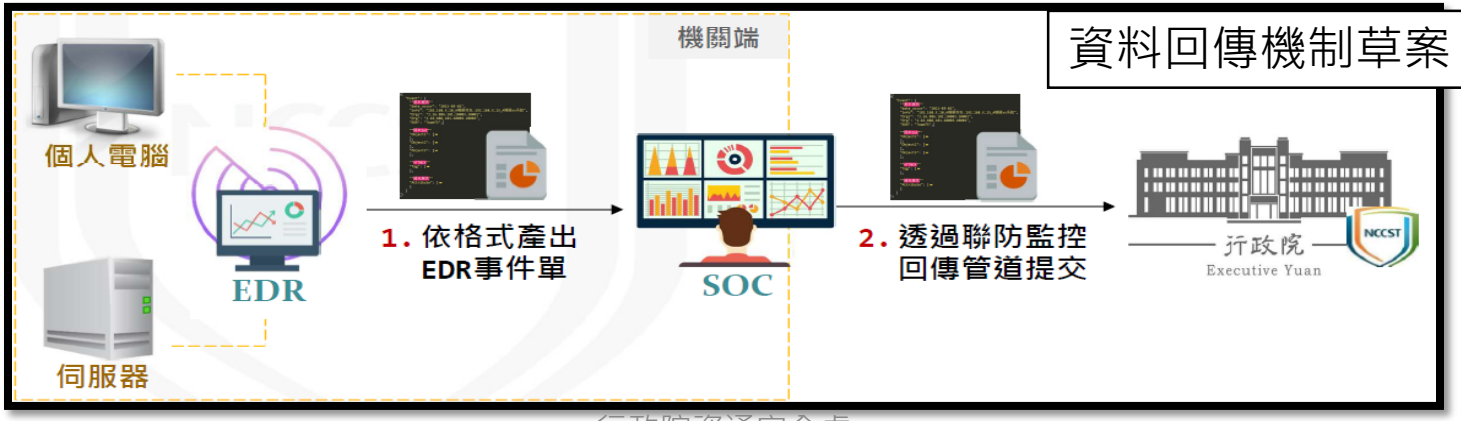
- 布建範圍為PC及主機，
  如受限資源，可根據重要性，逐年完成導入

□資料回傳機制(規劃中)

- 偵測到異常行為或惡意程式活動，並確認成為資安事件時，由EDR設備依格式產出事件單，並由SOC透過聯防監控資料回傳管道提交至主管機關

□相關作業

- 已於9月13日至15日舉辦機關說明會，後續將邀集共契上EDR相關廠商辦理說明會，針對配合事項與執行細節進行討論



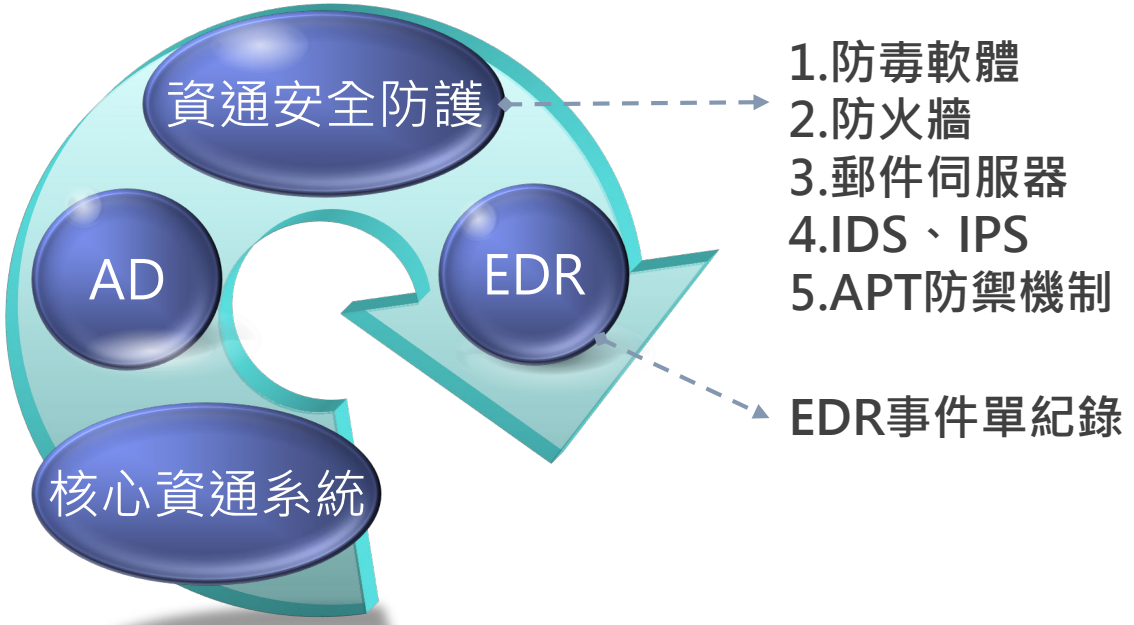
應辦事項-SOC監控範圍

制度面向	辦理項目	辦理內容
技術面	資通安全威脅偵測管理機制	▪ 初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料 ▪ 其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄

SOC監控必要範圍

1.資通設備紀錄

2.資訊服務或應用程式紀錄



應辦事項-專業證照、職能證書

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全專業證照及職能訓練證書	資通安全專業證照及職能訓練證書	一 初次受核定或等級變更後之一年內，至少四名資通安全專職人員，分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性 二 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定

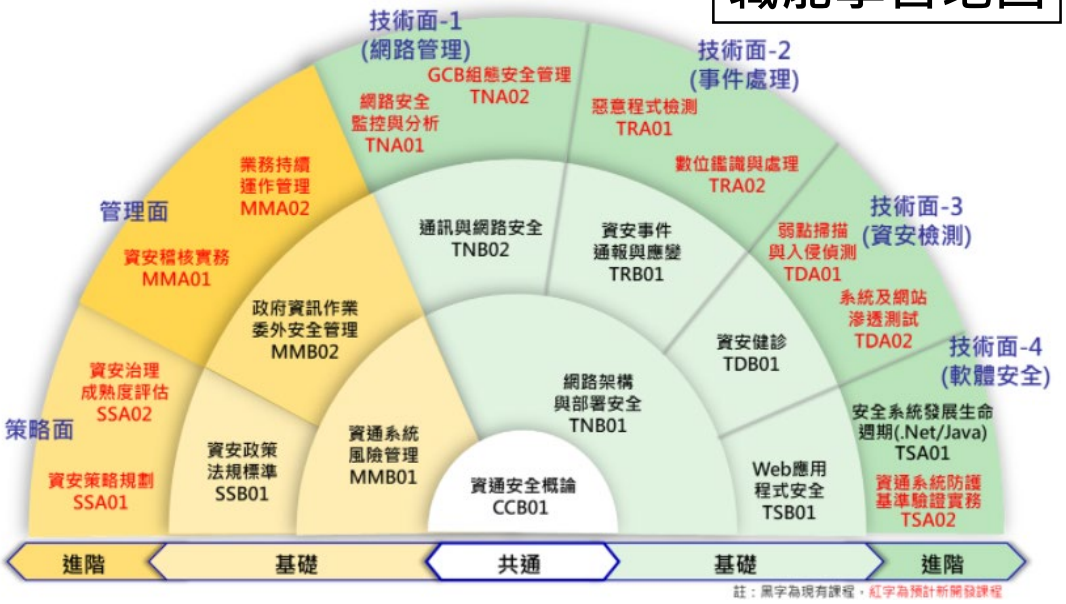
資安管理法

專業證照

日期 yyy/mm/dd

110-09-14	資通安全管理法及子法彙整版(1100914更新
110-08-23	「資通安全管理法施行細則」、「資通安全定非公務機關資通安全維護計畫實施情形稽通安全事項獎懲辦法」部分條文修正
110-07-28	110年第2季更新之資通安全專業證照清單

職能學習地圖



應辦事項-公正第三方驗證證書

備註：
二、「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；第三方核發之驗證證書應有前開委託機構之認證標誌

- 若機關已完成驗證之證書無TAF之標誌，可於年度追查時做轉證申請
- 有關轉證申請相關作業流程及費用，可洽各驗證公司協助說明、評估

Management System
Certification
MSooo

註：依資通安全責任等級分級辦法-C級以上機關應辦事項：
ISMS導入及驗證(B級以上)範圍為全部核心資通系統

防護基準-存取控制-遠端存取

□遠端存取

三、應監控遠端存取機關內部網段或資通系統後臺之連線

四、應採用加密機制

- 將現行高級及中級控制措施第一點及第二點規定事項移列為**普級控制措施**之第三點及第四點規定，並定明監控之類型為**機關內部網段**或**資通系統後臺**

機關遠端存取，至少應監控範圍

內部網段	資通系統後臺

行政院資安處110年3月2日
院臺護字第1100165761號函

遠端存取：「原則禁止、例外允許」

各機關開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「**原則禁止、例外允許**」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：

1.依資安法遠端存取相關規定辦理

2.以短天期為限

3.建立異常行為管理機制

4.結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如VPN)登入密碼

防護基準-系統日誌保留

□記錄事件

➢訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月

- 為使規範文義更為明確，爰將相關規定之「稽核」屬名詞者修正為「日誌」，屬動詞者修正為「記錄」
- 於記錄事件之普級控制措施，定明機關應訂定日誌之記錄時間週期及留存政策，並保留日誌**至少六個月**

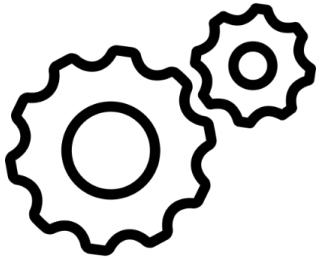
修改機關資通安全維護計畫或相關文件

跡證保存、根因調查

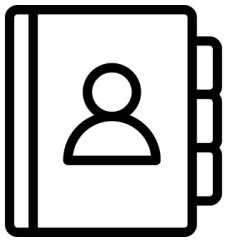
防護基準-資料儲存之安全

◘ 資料儲存之安全

➢資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存



重要組態設定檔(config、configuration)
個人電腦、印表機、應用程式、伺服器等



其他具保護需求之資訊
由機關評估其他應保護之資訊，如儲存機敏資料之DB欄位

資料庫加密

對具機敏資料之欄位或資料表進行加密，惟可能降低資訊系統運作效能，機關應先進行評估及測試效能影響程度

109年資通安全維護計畫實施情形

109年實施情形填報狀況

□ 實施情形未達成率較高項目(本院審查)

序號	項目
1	未確實盤點資通系統與服務
2	未依資通安全管理法規定，擬具對所屬機關資安稽核計畫並執行
3	未確實辨識機關核心業務及其重要性之盤點
4	未足額配置法遵要求之資安專職人力
5	未訂定情資分類評估及因應措施
6	未設置或參與其他機關之資通安全推動組織

□ 各級機關實施情形未達成率較高項目

A級公務機關	B級公務機關	C級公務機關	D級公務機關	E級公務機關
1.資安專責人員	1.資安專責人員	1.對所屬機關辦理實施情形稽核作業	1.訂定所屬機關稽核機制	1.設置或參與資通安全推動組織
2.對所屬機關辦理實施情形稽核作業	2.訂定資通安全情資之評估及因應機制	2.訂定所屬機關稽核機制	2.對所屬機關辦理實施情形稽核作業	2.資通安全風險評估
3.訂定所屬機關稽核機制	3.對所屬機關辦理實施情形稽核作業	3.資安專責人員	3.訂定資通安全情資之評估及因應機制	3.訂定資通安全情資之評估及因應機制

確實盤點資通系統與服務

建議

- 附表3「機關資通系統與服務資產清冊」盤點範圍
  - ① 業務使用(包含以勞務服務、行政協助或計畫補助等方式籌獲)之資通系統與服務
  - ② 自行或委外開發之資通系統與服務
  - ③ 暫無需提報：機關內電腦、手機、印表機等硬體設備，目前由各機關自行盤點及掌握
- 系統之盤點結果及異動情形應提報資安長知悉
- 應參考附表九「資通系統防護需求分級」之分級原則，訂定較客觀及量化之衡量指標(普中高)，使一致性分級

擬具對所屬機關資安稽核計畫並執行

建議

- 機關應依資通安全管理法第13條及第16條規定，稽核所屬/所管/所監督機關之實施情形
- 機關之稽核規劃，應包含所屬/所監督公務機關及所管特定非公務機關，如所屬/所管/所監督機關數量較多，可評估不同之稽核作法，如部分採書面、分層、橫向稽核等，由所屬機關分層平行或向下稽核，亦可考量機關等級及數量，決定適當稽核頻率

	已稽核所屬	未稽核所屬
A級機關	22	4
B級機關	62	19
C級機關	92	90
D級機關	50	86
E級機關	0	1

註：無上級機關之納管機關

核心業務及其重要性之盤點

□建議

- 依施行細則第7條規定，核心系統係指支持核心業務持續運作必要之系統或防護需求等級為高之系統，惟部分機關未將防護需求等級為高之系統，列為機關核心系統

支持核心業務**持續運作必要**之**系統**

核心系統

防護需求等級為高之系統，應為**核心系統**

組織規程

機關掌理事項如下：
1.OOOOO
2.OOOOOOOO
3.....

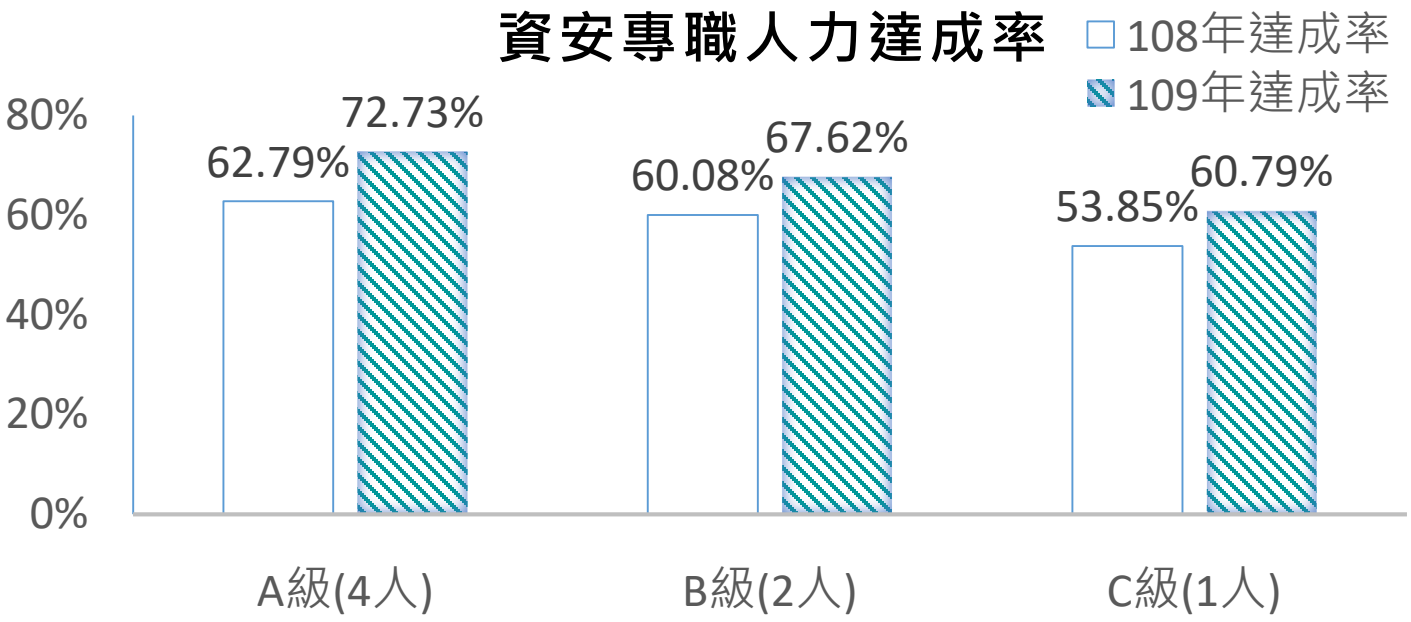
核心業務

系統名稱	系統屬性	版本類別	系統建置方式	系統主管機關名稱	系統管理者(部門)	系統使用者(部門)	主機設置於機關內	核心系統(Y/N)	含機敏資訊(Y/N)	防護需求等級
OO系統	業務	機關自用	自行委外				是	否	否	高

資安專職人力

□建議

- 各機關應優先於機關總員額配置資安專職人力，如仍暫無缺額人力可支配，得先以約聘僱或委外人員擔任
- 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，並依法調整資通安全責任等級，減少機關所應配置之資安專職人力



情資評估因應

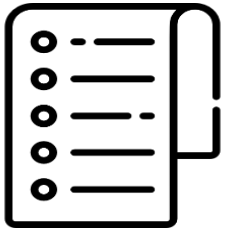
建議

- 機關可由行政院資安會報技術服務中心或其他管道接收資安情資(如：軟體弱點通報、惡意中繼站清單)，並針對接獲之情資，進行分類評估及因應措施(如：弱點修補更新、封鎖惡意中繼站IP)

接收軟體弱點通報

盤點掌握

弱點修補/強化防護



接收惡意中繼站清單

封鎖惡意中繼站IP

資通安全推動組織

建議

- 機關應成立或參加其他(上級)機關的資通安全推動小組，且成員應涵蓋各單位，提升參與成員職級至單位副主管以上之人員，並定期開會，於會議中檢視機關資通安全政策及目標、各資安防護作業、稽核機制、資通安全事件通報、應變與演練等相關法遵事項辦理情形

資安治理成熟度

第六期國家資通安全發展方案目標

- 113年所有A級政府機關
- 80%之B級政府機關資安治理成熟度達第3級以上

預期效益

- 分析機關資安防護弱項，據以爭取資源以提升機關資安防護能量
- 陳報自評結果與改善方案，供機關首長與資安長了解機關資安概況

110年新增指標調整說明(110年9月說明會)

1. 政府領域資安聯防情資
   - 回傳情資涵蓋之資安防護項目
2. 政府資安警訊
   - 收到之資安警訊，對應資安事件影響等級加權計分
3. 資安事件通報逾時
   - 依通報**逾時**情形(無資安事件，不列入計分)

資通系統防護基準驗證實務參考指引

資通系統防護基準驗證實務參考指引

- 針對資通安全責任等級分級辦法附表10「資通系統防護基準」，說明7個構面、29項控制措施類別之各項控制措施，逐項說明其控制措施、使用等級、內容說明及驗證實務等，並提供可能之佐證資料作為驗證之參考依據

資訊人員

- 了解防護基準所訂各項控制措施應辦理內容，據以參考執行
- 參考本指引所提供之驗證實務作法，透過自評確認控制措施是否落實執行

資安人員

- 於內外部稽核時，參考本指引所提供之實務作法，驗證資通系統之各項防護措施，是否符合資通系統防護基準之規定

可至「技服中心網站/共通規範/參考指引」下載

資通系統防護基準驗證實務-範例

	控制措施	**對日誌之存取管理，僅限於有權限之使用者**
	適用等級	普、中、高
資訊人員	**內容說明**	**日誌應妥善留存**，以符合程式除錯、行為歸責、稽核取證及法律規範等使用需求，且其中可能存在機敏資訊，故應**禁止未授權的存取、刪除及修改**。應**施行日誌(及其備份)之存取控管**，僅限有權限之特定人員(如系統或資料庫管理者等)存取日誌(如日誌檔案或日誌主機等)，以保護機密性、完整性及可用性，此存取控制可能利用實體安全、系統功能實作帳號與權限管理或其他適用之管控機制來達成
資安人員	**驗證實務**	▪ 如未針對資通系統日誌進行存取管理，或允許非權責人員任意調閱，則未符合此控制措施 ▪ 驗證人員宜**檢視機關訂定之日誌相關管理辦法**，並**訪談相關權責人員**(如系統管理者與資料庫管理者等)，以了解機關如何針對日誌進行存取管理 ▪ 驗證人員宜**發展測試案例以驗證**存取控制之有效性，**如嘗試利用未授權存取之使用者帳號存取日誌，應能有效禁止**其存取行為，例如，若機關規定僅限資料庫管理者存取留存於資料庫之日誌內，則驗證人員可驗證系統管理者或一般使用者帳號無法存取日誌
	佐證資料	▪ 機關訂定之日誌管理辦法 ▪ 日誌存取控制權限申請/審核紀錄 ▪ 存取日誌之測試紀錄

資料來源：節錄參考指引第51頁

資通系統防護基準檢核表-範例

- 於內外部稽核時，資安人員可藉由本參考指引所附檢核表逐項進行驗證符合與否

安全控制措施	符合性	符合性或不適用情況說明	複查結果/佐證資料
建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	符合	依「ISMS_WI_016網站管理辦法」之規範，網站管理帳號變更/新增之申請，需填寫「流程服務管理系統」之「系統帳號/權限異動申請表」，由網站管理者進行變更/新增作業。	1.系統帳號/權限異動申請表」 2.帳號權限審核紀錄
已逾期之臨時或緊急帳號應刪除或禁用。	符合	1.臨時帳號建立時由系統設定帳號使用截止日期，逾期自動禁用。 2.每季進行系統帳號權限審查。	1.系統功能規格書/測試記錄 2.帳號權限審核紀錄
資通系統閒置帳號應禁用。	符合	1.系統實作每日檢查排程，自動禁用逾180未登入之帳號。 2.每季進行系統帳號權限審查。	1.系統功能規格書/測試記錄 2.帳號權限審核紀錄
定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。	符合	每季進行帳號權限審查。	帳號權限審核紀錄
機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。	符合	系統設定操作閒置時間20分鐘自動登出，無限制使用時段。	伺服器組態設定
逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。	符合	系統設定操作閒置時間20分鐘自動登出。	伺服器組態設定
應依機關規定之情況及條件，使用資通系統。	符合	資通系統僅限使用自然人憑證登入。	系統使用手冊
監控資通系統帳號，如發現帳號違常使用時回報管理者。	符合	部署WAF防護設備，偵測及阻擋站台惡意使用行為。	WAF組態設定

建議由承辦人員預填後，再由資安人員確認

資料來源：節錄參考指引附件

資安強化措施(委外管理)

委外管理資安強化規劃(草案)

籌獲階段

- 系統籌獲文件，應標註系統防護需求等級
- 籌獲案明列資安經費

規劃中之強化作業

- 評選項目：資安作業(乙方自評)及受託者經歷
- 資安專業外部委員
- 資安評分佔比：至少佔總分10%(資通系統/服務經費佔比低於全案10%者，至少佔總分5%)

建置階段

強化系統驗證及廠商稽核

- 防護基準驗證指引
- 委外廠商稽核準則

規劃中之強化作業

- 系統開發應有機關資訊/資安人員參與確認
- 資安專業外部委員於決標後轉任機關資安顧問
- 重要資通系統應評估引入獨立驗證及認證機制

維運階段

- 機關應優先**配置資安專職人員**，檢視並確認落實資安管理措施
- 受託者應**配置資安專職人員**，確認履約階段符合雙方資安管理規範
- 受託者應**自行辦理資安稽核作業**，定期對受託者辦理資安稽核

視訊與即時通訊軟體使用安全注意事項

視訊會議使用注意事項(1/2)

- 各機關建置視訊會議軟體，得使用商用軟體、自行採購雲端服務或自行建置等方式辦理，並應**優先**自**共**同供應**契**約進行採購
- **產品選用**評估項目
  - 應瞭解使用產品之**傳輸及儲存機制**，不得有連線至中國大陸(含港、澳)IP等網路行為
  - 產品視訊會議之傳輸連線應有**安全加密**機制
  - 視訊會議應具**安全管理**機制，如提供帳號、密碼登入權限或二階段登入等功能，避免非必要人員連線
  - 產品如有弱點被揭露，供應商應提供**修補**程式並即時**更新**

視訊會議使用注意事項(2/2)

- **同仁使用宣導**事項
  - 會議召集方，應加設**會議室密碼**，並注意會議錄音(影)**功能設定**
  - 進行**會議錄音(影)**時，應確保資料係**存放**在使用者端或指定之安全地點
- 如因**會議主辦方**採用具資安疑慮產品，可採行以下措施
  - 採**專機專用**模式，使用非處理且無公務資料之電腦設備
  - 會議過程應確保**不使用及連通公務網路**(含內、外網)
  - 使用**WEB版**用戶端界面，瀏覽器套用政府組態基準(Government Configuration Baseline, **GCB**)，以**無痕模式**連結使用
  - 如必須安裝本機端視訊軟體，會議結束應將使用之電腦**設備**執行**格式化**

即時通訊軟體使用注意事項(1/2)

- 各機關**建置**即時通訊軟體，得使用商用軟體、自行採購雲端服務或自行建置等方式辦理，並應**優先**自**共**同供應**契**約進行採購
- 各機關得視整體資通安全風險及業務需求，**另訂不宜傳遞之機敏訊息**
- **產品選用評估**
  - 訊息於**傳輸**過程應有**安全加密**機制
  - 伺服器端之**主機設備**及**通訊紀錄**應置於我國**境內**，或產品使用過程中**不得有連線至中國大陸(含港、澳)IP等網路**行為
  - **產品原始碼(source code)不得有屬中國大陸(含港、澳)者**
  - 伺服器端通訊紀錄**(log)應至少保存6個月**
  - 應通過經濟部訂定之「基本資安檢測基準**行動應用APP**」之**L2檢測**
  - 產品如有弱點被揭露，應確認供應商提供**修補**程式並即時**更新**

即時通訊軟體使用注意事項(2/2)

同仁使用宣導事項

- 應謹慎使用公開之無線網路，並留意藍牙、衛星定位系統及近場通訊等**連線安全**
- 於未確認傳遞者身分前，**不得任意**點選訊息之**超連結**，並注意釣魚、惡意或高風險之網站服務
- **不得傳遞隱私或未經證實之訊息，**但未經證實之訊息須釐清或有其他業務需求者，不在此限
- **人員離(調)職**時，應**退出**原任機關各即時通訊**群組**，並**刪除對話紀錄**；對前揭資料及帳號資訊，**應予保密**

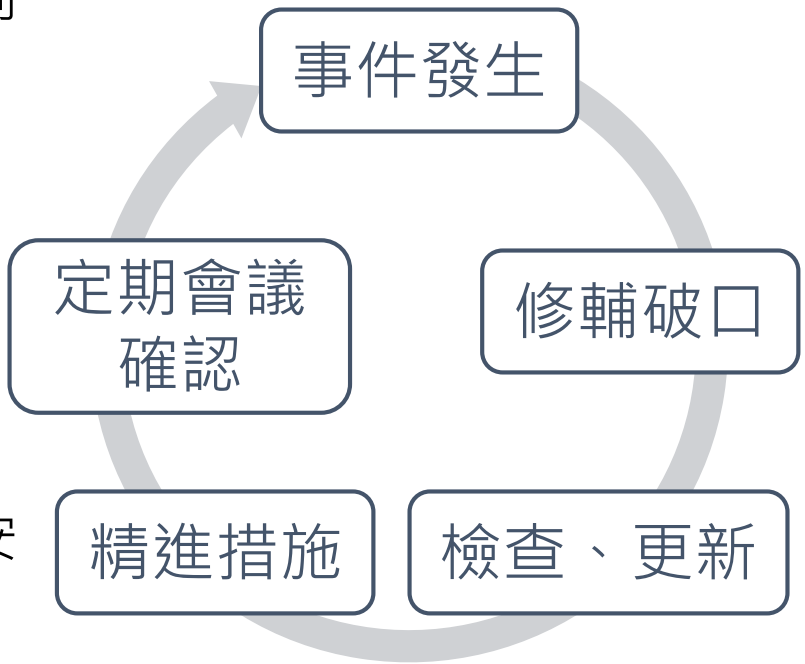
事件應變案例宣導

事件應變案例宣導-結案不等於改善

- 某機關多次對外發起異常連線，後續發現遭植入多個惡意程式，而機關每次接獲警訊，僅就警訊所提惡意中繼站進行阻擋

➢ 原則一：落實事件調查

- 以掃描軟體、EDR、SOC等方法找到植入方式，確實修補資安破口
- 檢查同網段是否有異常行為或檔案
- 除持續監測外，也應該要完成更新



➢ 原則二：個案看通案

事件結案≠改善完成

- 從前述調查結果找出破口，歸納資安管理精進措施
- 視精進措施調修管理規範，並定期會議確認辦理情形

弱密碼議題宣導

弱密碼議題宣導

- 110演練機關，攻擊報告43%為弱密碼，行政院資安處105年11月30日院臺護字第1050185463號函，各政府機關資訊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

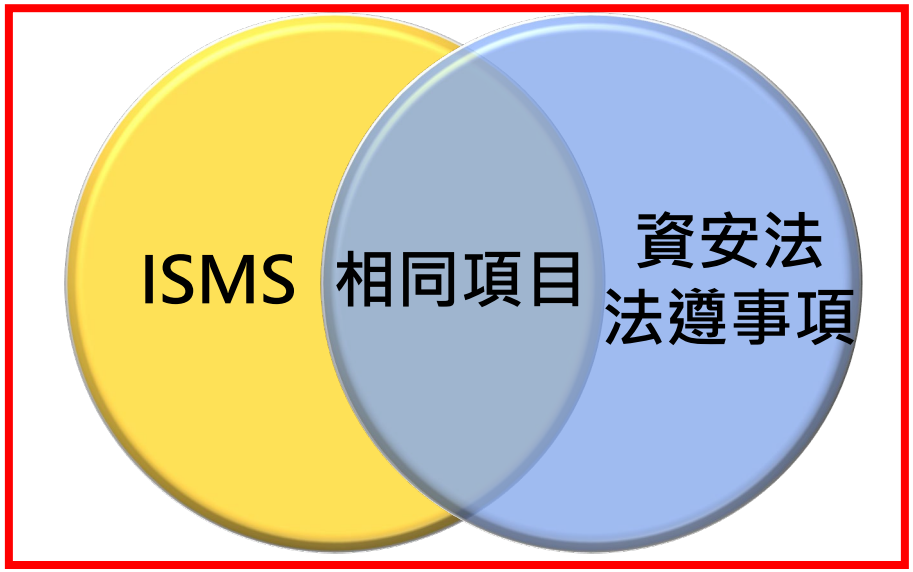
1.建議可比照GCB套用之Windows密碼原則規定，限制機關人員密碼複雜度設定

2.強化通行碼設定原則

資通安全管理法驗證方案(草案)

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」**，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

資安法驗證方案實施方式

- 資安法驗證方案**追加稽核項目**如下
  - **資安維護計畫/實施情形**
  - **資安責任等級應辦事項**
  - **資通系統防護基準**
- 驗證範圍內之**資通系統**，應至少包括下列相關**人員**(含輪班與委外駐點)
  - **系統操作維運者**：機房、網路、設備等操作管理與維修、作業系統管理、資料庫管理等
  - **資通系統開發維護者**：程式設計師、分析師、整合/架構師等
  - **資通系統使用者**：對資通系統具有新增、刪除、修改之部分或全部權限者

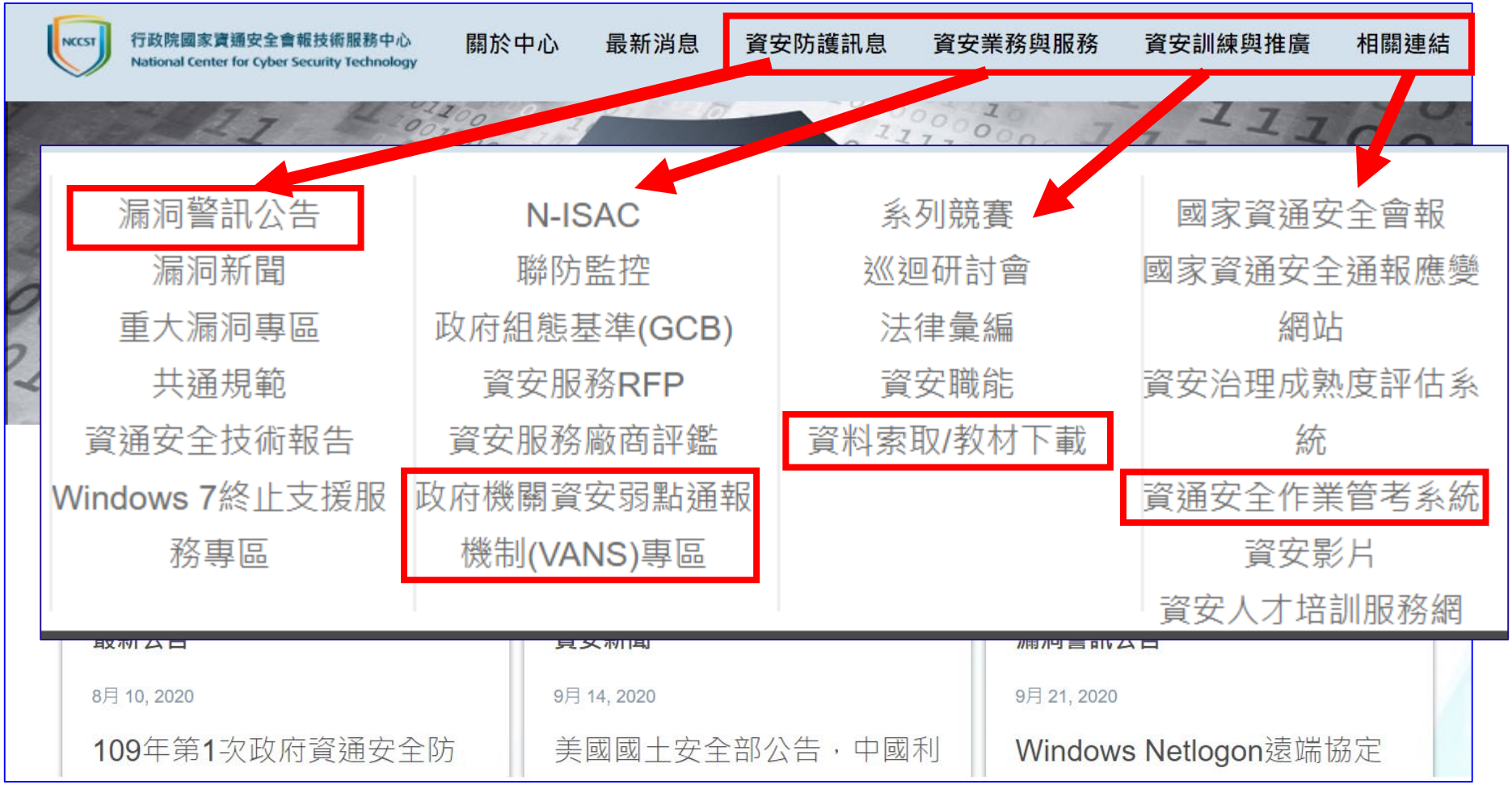
參考資訊

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