資通安全業務重點工作

114年11月

大綱

一、資安政策與治理
- 《資通安全概論》職能訓練教材改版
- 政府組態基準(GCB)設定
- 新版VANS系統作業推動
- 建立資安專職人力調訓機制
- 資安業務績效評核

二、資安技術與防護機制
- 持續精進網路攻防演練
- 受託者資通安全聯合查核指引

三、近期政府機關資安事件案例分享及資安宣導

一、資安政策與治理

《資通安全概論》職能訓練教材改版

《資通安全概論》職能訓練教材改版

以資安法為主軸，並**以書籍式呈現**

114年11月28日起

於「資安人才培訓服務網」**開放新版教材下載**

115年3月

訓練機構採用新版教材**辦理資安職能訓練**

115年6月

配合資安法子法修法，教材調修納入相關內容

115年9月後

規劃製作數位課程，上架e等公務園提供線上學習管道

11月 — 3月 — 4月 — 6月 — 9月

類別		報考資格	報考區間
免訓評量		1. 科目限**《資通安全概論》，需提出申請（申請方式115年2月公布）** 2. 比照參訓評量，1次首測+4次複測(複測仍須收費300元)	申請免訓評量後1年內
參訓評量	首測	1. 參加該科目資安職能訓練 2. 訓練出席率達五分之四以上	自結訓後1年內
	複測	1. 已參加首測評量，惟成績未達合格標準 2. 報考以4次為限，每次收費300元	
	換證	1. 已持有資安職能訓練證書 2. 報考以2次為限	證書效期截止日(含)前6個月內

115年4月

- 依新版教材完成**評量題目改版，通過該評量取得之證書效期延長為5年**
- **開放免訓評量**

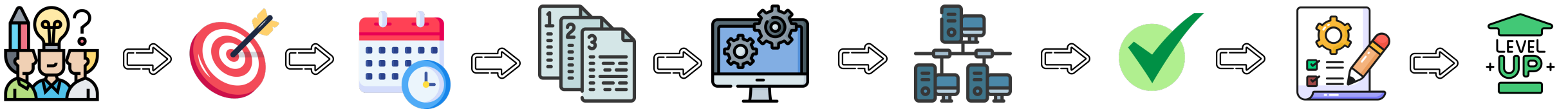
已持有概論證書者，於證書效期到期前參加換證評量即可，無需配合改版換證，但**換證試題配合新版教材更新**

推動政府組態基準(GCB)設定

推動政府組態基準(GCB)設定(1/2)

- ✓ 資安責任等級A、B級公務機關應於初次受核定或等級變更後之1年內，依主管機關公告之項目，**完成GCB導入作業，並持續維運**；主管機關**如有新增公告項目**，亦應就該項目**於公告1年內完成導入**。
- ✓ 已公告項目涵括作業系統、瀏覽器、網通設備、應用程式等4類，115年第4季預定新增第5類雲端服務(逐步發展大型公有雲GCB)。
- ✓ 機關針對**所有已公告項目均應評估導入**，並留下紀錄，導入**採「專版專用」原則**，導入前應**先充分測試**，且依實務需求辦理例外管理。
- ✓ **例外管理項目須落實定期檢討與審核**；**已導入項目建議納入資安健診驗證**。

導入作業流程



建立團隊 → 確認目標 → 規劃時程 → 專版專用 → 單機測試 → 小規模測試 → 結果驗證 → 納入程序書 → 提升資安防護

推動政府組態基準(GCB)設定(2/2)

已公告新增項目

- Palo Alto Firewall 11 (網通設備)
- Microsoft IIS 10 (應用程式)

預訂新增項目

- Mac OS (作業系統)
- Amazon Web Services (雲端服務)
- Fortinet Fortigate 7.x (網通設備)
- Safari (瀏覽器)

逐年發展市佔率較高之公有雲，如Microsoft Azure及Google Cloud Platform(GCP)等

114年第4季 → 115年第4季

新版VANS系統作業推動

新版VANS系統作業推動

- 新版VANS系統已於9/1上線，請C級以上公務機關與CI提供者配合導入
- 修正VANS相關推動作業事項(自10/1起適用)

盤點資料上傳頻率

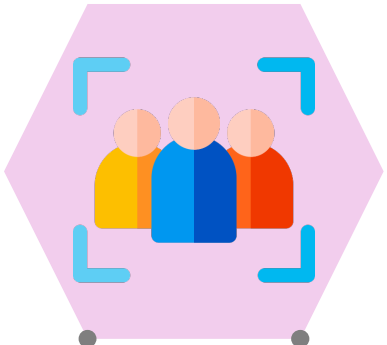
針對資訊資產盤點資料上傳頻率，建議**每季至少上傳1次**以比對弱點資訊。

弱點修補或防護配套並持續管理

高風險(CVSS 7.0分以上)弱點，應優先修補；如未能即時修補，應於完成修補前規劃緩解措施，加強監控、防護配套及異常偵測。相關弱點處置方式或改善措施，建議每季完成比對弱點後**1個月內**，至VANS系統（更新）填寫，**強化機關弱點管控作為**。

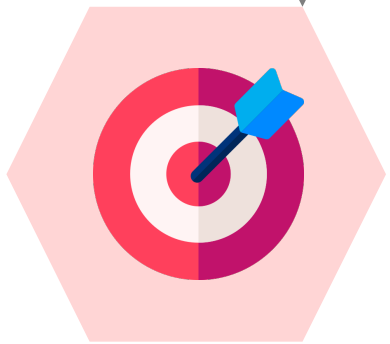
建立資安專職人力調訓機制

建立資安專職人力調訓機制



對象

- 公務機關資通安全**專職人員** (A級4人、B級2人、C級1人)
- 人數規模約**1,500**人，原則均應實體參訓



目的

- 透過**年度調訓**，持續強化資安人員防護專業知能
- 協助資安人員**瞭解政策推動重點**與**提供防護建議**
- 增進各機關資安人員間之**交流互動**，凝聚社群力量

辦理方式

- **自115年起，資安防護巡迴研討會併入資安專職人力調訓活動**
- 每場次**活動規劃1天**，採**多元形式辦理**，如講座論壇、工作坊、團隊遊戲等
- 上午為**共通性課程**，下午**依職務分眾規劃交流性活動**

資安業務績效評核

資安業務績效評核宣導(1/2)

受評對象

機關

資通安全責任等級B級以上中央機關(構)、公法人、直轄市政府所屬資訊機關及縣(市)政府。

※ 直轄市政府所屬資訊機關係指主要負責直轄市政府整體資通安全業務、管理及推動之機關，且以1個為限。

組別	類別	所屬機關
1	**A級**中央機關(構)及公法人	無
2		有
3	**B級**中央機關(構)及公法人	無
4		有
5	B級以上之**直轄市政府所屬資訊機關**及**縣(市)政府**	有

(均列入評選)

人員

資通安全責任等級C級以上公務機關之專職辦理資通安全業務現職公務人員、聘用人員及約僱人員。

※各機關依現有公務人員總人數遴薦人員。**(採機關遴薦報名制)**

機關現有公務人員總人數	未滿500	500-1000	滿1000（其後每滿1000）
得遴薦人員數量	1	2	3（+1）

資安業務績效評核宣導(2/2)

評核項目

1. 資通安全管理法法遵應辦事項執行情形
2. 資通安全管理作業及業務配合執行情形

→ 依機關平時表現評分，占總分85%

3. 其他資通安全管理業務促進活動或特殊創新作為

→ **依機關提交之書面報告評分， 占總分15%：**

- 機關：未提交則不計分
- 人員：未提交則視為未遴薦人員參加

獎勵方式

類別	獎勵條件		獎勵金	獎座
機關	以受評機關20%為限	優等以上	114年，7萬5,000元/每機關 依預算最高可達30萬元/每機關	1座
		良等	無	
人員	取受評人員評核成績前20%者		114年，1萬元/每人 依預算最高可達5萬元/每人	1座

請各機關踴躍提交書面報告，爭取獲得佳績及獎勵

二、資安技術與防護機制

持續精進網路攻防演練
(簡報將於現場投放)

受託者資通安全聯合查核指引修正

「受託者資通安全聯合查核指引」後續修正重點

- ✓ 行政院於110年12月14日函頒「受託者資通安全聯合查核指引」，經試行一年期滿。
- ✓ 本次修正重點以**擴大稽核涵蓋範圍及強化技術面合規事項**為目標，以分層為原則，納入主管機關及公務機關聯合辦理之參考作法，供機關參考。

建議作法

資安法主管機關籌組稽核團隊

公務機關依據資訊服務採購契約，**委由資通安全管理法主管機關籌組專案團隊稽核**

公務機關自行籌組聯合稽核團隊

- **中央二級機關聯合所屬三、四級機關或聯合同領域公務機關**
- **地方政府得參照上述辦理**

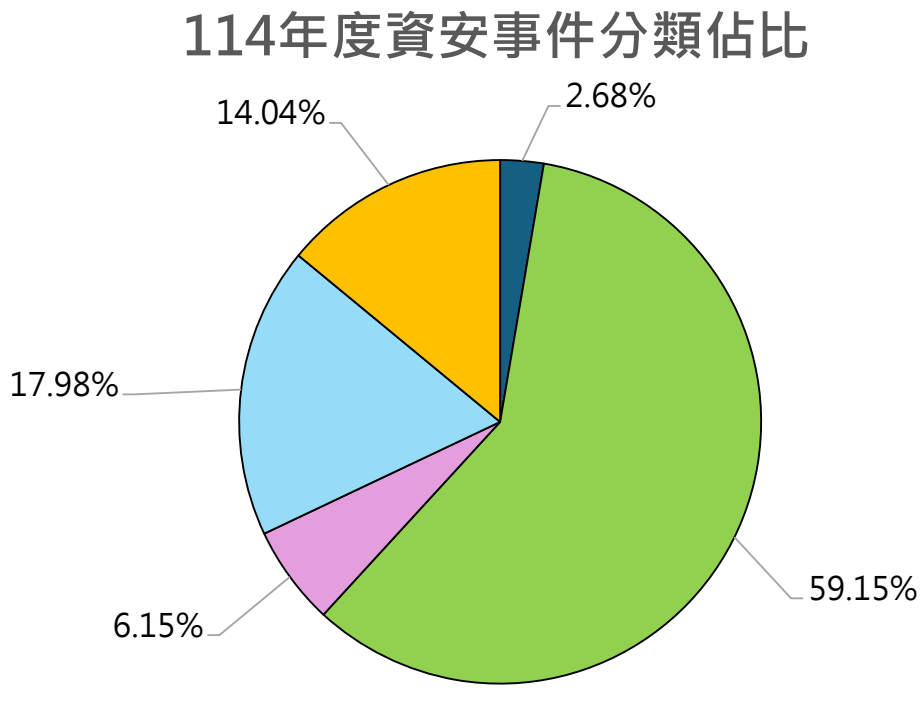
三、近期政府機關資安事件案例分享及資安宣導

近期政府機關資安事件案例分享

114年1月至9月資安事件(1/5)

納管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
114年(1-9月)	634	529	80	**25**	0



設備問題

主因：多為設備異常/毀損、電力供應異常等

非法入侵

主因：為使用/下載來源不明之應用程式/套件，**主要為下載含有惡意程式之偽冒通訊軟體**

114年1月至9月資安事件(2/5)

3級以上資安事件樣態

機密性
(共12件)

- 雲端空間權限設定不當
- 人員疏失
- 社交工程
- 公文系統設定錯誤
- 網頁漏洞遭利用

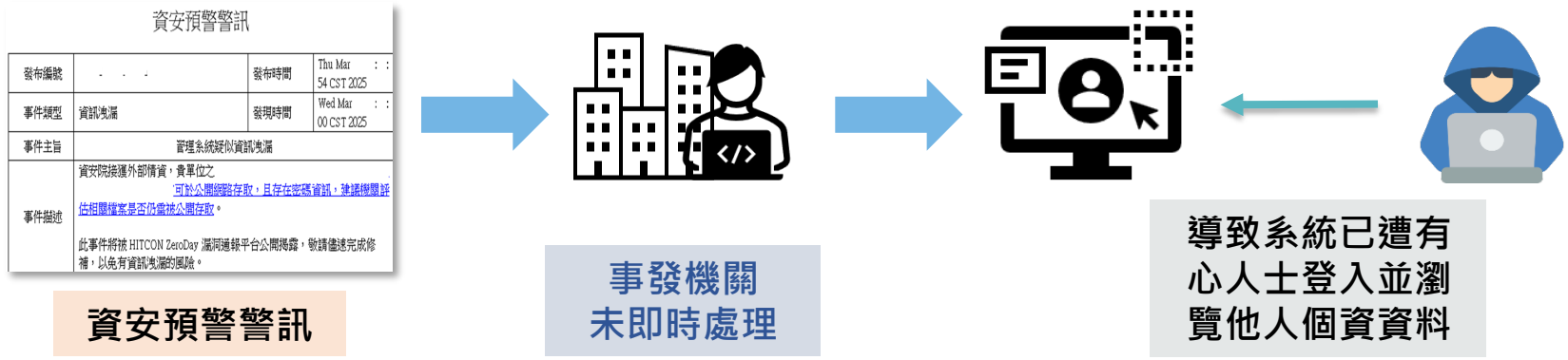
可用性
(共13件)

- 電力問題核心系統可用性中斷
- 系統遭入侵，影響核心業務(急診業務)
- 目錄權限設定錯誤，影響機關CI核心業務可用性
- 資料庫異常，無法於可容忍中斷時間內修復
- 網路設備異常，影響機關CI核心系統可用性

114年1月至9月資安事件(3/5)

未即時處理資安預警警訊導致個資外洩

- 案係本署於114年3月發布**資安預警警訊(EWA)通知機關系統疑似存在弱點**，請機關儘速確認並進行必要應處，**惟機關遲至5月被通知後才進行處理，該系統已遭有心人士登入並瀏覽他人個資資料**，已造成個人資料外洩風險，爰通報3級資安事件。



建議防範措施

- 本署及資安院發布之EWA警訊，機關應儘速處理，**並依警訊內容進行檢視，若發現入侵事實(機密性、完整性或可用性受影響)，須依資安法進行通報**
- 資料保護，敏感資料加密儲存、**查詢過程遮蔽及最少揭露**

114年1月至9月資安事件(4/5)

雲端空間權限權限設定不當

- 機關辦理參訪活動報名時，透過QR CODE供民眾至雲端空間下載報名表，後續廠商將整理後含個資之報名資料與民眾可下載報名表存放於相同雲端空間內，**惟未設定雲端空間存取權限，導致民眾可掃描QR CODE後下載含個資之報名資料**，致敏感資訊外洩。

建議防範措施

- 機關辦理對外活動或公告所使用之報名方式時，**應確認其內容之妥適性及其資安管理措施**，避免因設定不當致資料外洩
- 使用雲端空間分享敏感資訊時，**檔案需加密，且資料夾應有合適權限管控**
- **注意廠商管理**，針對機敏資訊應加強管理與防護

114年1月至9月資安事件(5/5)

機關公務電話節費盒遭入侵及盜撥電話

- 案係某機關發現其公務電話遭不明人士盜打進行詐騙，經查該**公務電話係機關使用之網路電話**，比對撥話紀錄，發現有外部IP撥打情形，判斷應係設置於**機關內部之電話節費盒遭外部惡意登入**後，進行未授權撥號所致。

建議防範措施

- **使用高強度密碼**、並定期更新以及移除預設帳密
- **遵循「原則禁止，例外允許」原則**，進行存取限制管理
- 納入監控，**定期查看帳號登入及設備連線記錄**，避免異常情形
- **定期盤點更新狀態**，若設備已停產或不再提供安全性更新，應評估是否需進行汰換

資安宣導

資安宣導(1/2)

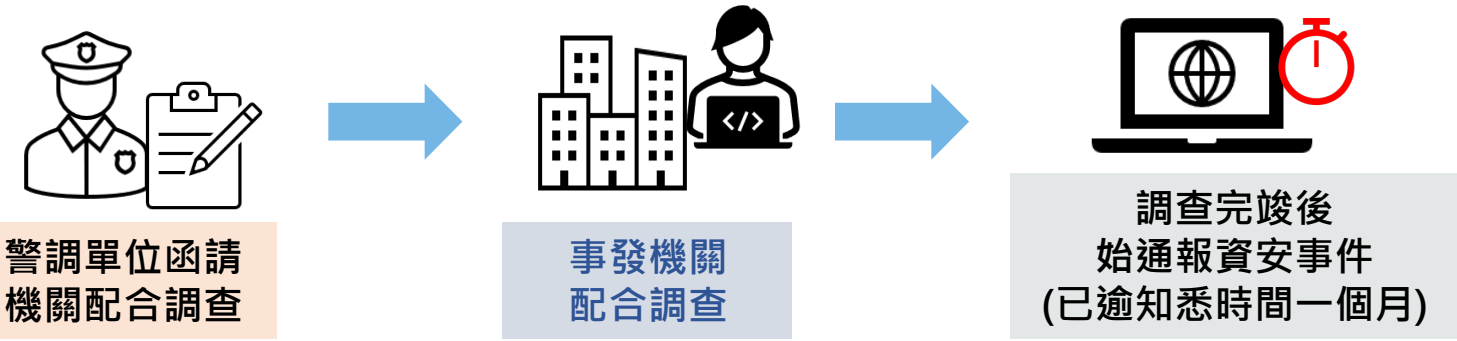
資安推廣-惡意檔案檢測服務

本署所管**台灣電腦網路危機處理暨協調中心(TWCERT/CC)，提供惡意檔案檢測服務(VirusCheck)**，本服務採用雲地混合架構，利用公有雲具彈性、高效及安全等特點，並結合地端商用沙箱之分析能力確保檢測資訊不外洩。**建議機關可多加利用**，避免機關利用**VirusTotal**進行檔案檢測時，誤將敏感資訊上傳造成資料洩漏。

資安宣導(2/2)

配合偵查時仍須注意通報時效

- 警調單位通知機關疑似遭駭客入侵作為攻擊跳板，請機關配合對相關設備進行**主機鑑識**、**磁碟映像檔製作**及**網路封包側錄**等現地調研工作，並**注意保密，勿洩漏調卷資訊**。
- 機關配合調查工作，並於調查工作完竣後，始通報資安事件。



建議措施

- 機關於接獲警調單位通知疑似資安事件後，除配合進行調查工作外，於知悉(即確認)為資安事件後，仍須於時限內完成事件通報。
- 如無法確認通報內容，可與警調單位討論後通報。

資安是持續精進的風險管理