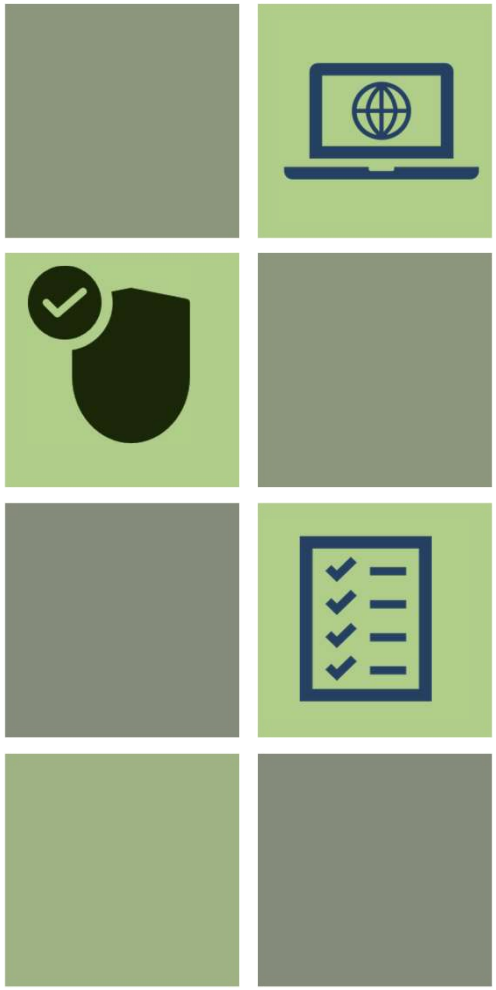
資安推動重點工作

113年6月

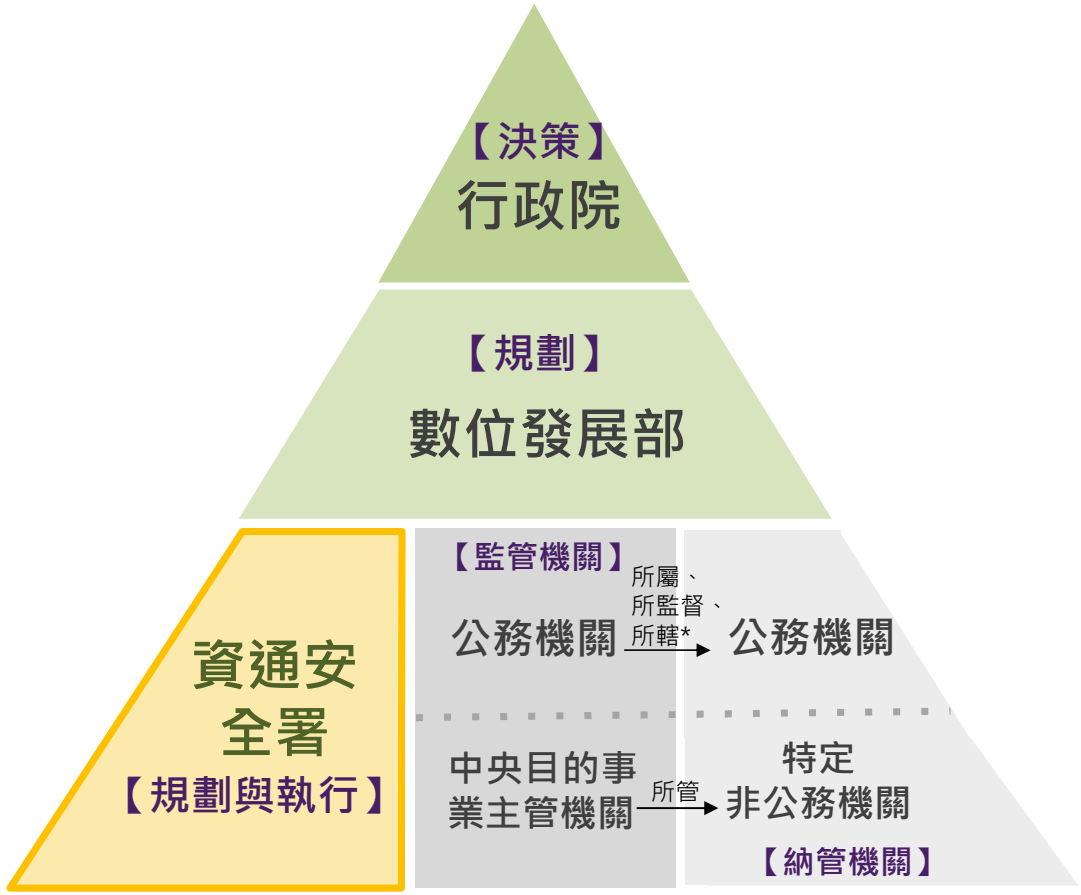


簡報大綱

- 壹、我國資安體系架構與權責
- 貳、112年實施情形概況
- 參、重點工作
  - -1.危害國家資通安全產品限制使用
  - -2.資安專職人員專業訓練規劃
  - -3. 零信任推動機制
- 肆、資安稽核及網路攻防演練常見發現

壹、我國資安體系架構與權責

我國資安體系架構與權責(1/2)



【註】所轄公務機關：在直轄市政府係指直轄市山地原住民區公所及直轄市山地原住民區民代表會；在縣(市)政府係指鄉（鎮、市）公所、鄉（鎮、市）民代表會

我國資安體系架構與權責(2/2)

資安架構

國家資安業務規劃與執行

溝通協調各部會

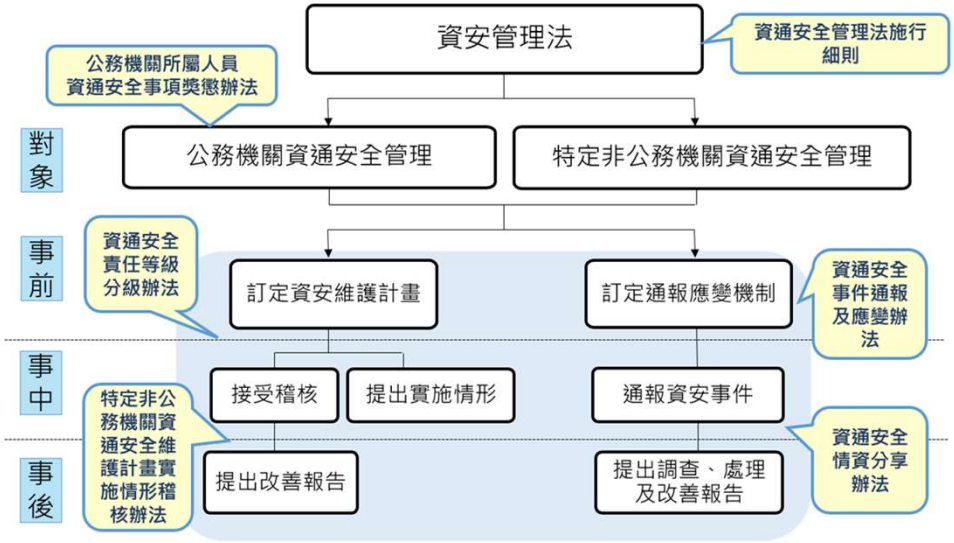
行政院國家資通安全會報

(本部為幕僚單位)

政策面
國家資通安全發展方案

願景	打造堅韌安全之智慧國家			
目標	• 成為亞太資安研訓樞紐 • 建構主動防禦基礎網路 • 公私協力共創網安環境			
推動策略	吸納全球高階人才培植自主創研能量	推動公私協同治理提升關鍵設施韌性	善用智慧前瞻科技主動抵禦潛在威脅	健全智慧國家資安提升民間防護能量
具體措施	1.擴增高教資安師資員額與教學資源 2.挹注資源投入高等資安科研 3.培育頂尖資安實戰及跨域人才	1.建立各領域公私協同治理運作機制 2.增強人員資安意識與能力建構 3.公私合作深化平時情資交流與應變演練	1.賡續推動政府資訊(安)集中共享 2.擴大國際參與及深化跨國情資分享 3.制敵機先阻絕攻擊於邊境 4.提升科技偵查能量防制新型網路犯罪	1.輔導企業強化數位轉型之資安防護能量 2.強化供應鏈安全管理 3.建構安全智慧聯網

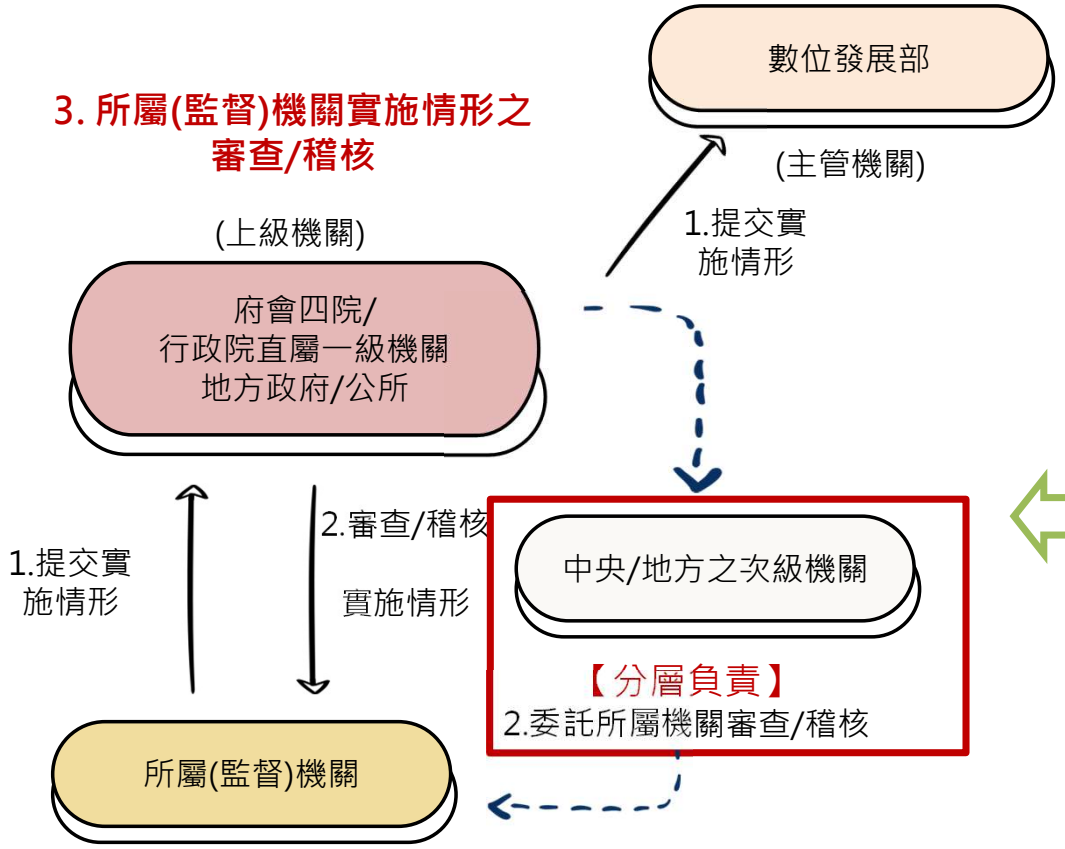
法遵面
資通安全管理法及6個子法



貳、112年實施情形概況

資安維護計畫【實施情形】審查及稽核

依資通安全管理法第12及13條規定



Q：針對所屬機關數較多之上級機關應如何落實審查及稽核作業？

建議可採**分層方式**，由上級機關委託所屬機關分層協助審查，並由上級機關**統籌及掌握所屬機關之審查/稽核情形**

資安維護計畫【實施情形】審查及稽核

112年度上級機關針對所屬機關實施情形審查作業

數位發展部資通安全署資通安全作業管考系統

實施情形(112)-填寫狀態總表-機關或下屬機關；預設登入機關排第一順位

##	機關OID	機關名稱	等級	公務機關/特定非公務機關	機關屬性	全部完成	實施檢核表	附表1	附表2	附表3-1、3-2	附表3-3	應辦檢核表	最後填寫機關	審核狀態	審核更新日期	應填報項目	特殊功能
1	[redacted]		A	公務機關	中央機關	未完成	填寫中	未完成(4人、15證)	已完成	未完成(6筆)	未完成(687筆)	未填寫	[redacted]	未審核			檢視(友善列印) 審核(上級使用)

審核功能

實施情形檢核表-審核意見

實施情形

流水編號：1061
被填寫機關OID [redacted]
被填寫機關OID

實施項目	實施內容	辦理情形	審核意見
1.核心業務及其重要性	1.1核心業務及重要性盤點？ 註：有關核心業務及核心資通系統之定義，請參考資通安全管理法施行細則第7條	◉盤點機關核心業務計 4項 ○未盤點機關核心業務，原因為： 補充說明(選填)：	

審核意見

針對所屬機關**審查情形**將列為資通安全業務**績效評核加分項目**

資料來源：管考系統112年實施情形

資訊資產設備盤點情形

各機關資通安全維護計畫應包含資通系統及資訊之盤點，應增列提報「**機關資通訊設備清冊**」，經統計112年各機關資訊資產提報資料，1%未登載廠牌，約30%設備未登載廠牌及型號

##	流水編號	設備名稱	廠牌名稱及型號	數量	備註
4491	710592	防火牆		0	
4492	710591	網路負載平衡器		0	
4493	710590	骨幹網路交換器(ACI)		0	
4494	710589	交換器		0	
4495	710588	網路認證管理系統		0	
4496	710587	路由器		0	
4497	710586	個人電腦	個人電腦	1	
4498	710585	平板電腦	華為	1	

錯誤樣態一

未包含廠牌資訊及型號

錯誤樣態二

資產設備數量確認

錯誤樣態三大陸廠牌未納入「大陸廠牌資通訊產品盤點」作業

參、重點工作

- 危害國家資通安全產品限制使用
- 資安專職人員專業訓練辦理規劃
- 零信任推動機制

危害國家資通安全產品限制使用原則

禁用陸牌規定

- ✓ 現階段係請各公務機關依行政院秘書長109年函，禁止使用及採購大陸廠牌資通訊產品(含軟體、硬體及服務)。
- ✓ 大陸廠牌認定係依行政院公共工程委員會107年函釋，所稱「大陸地區廠商：大陸地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體」所提供之產品。

!! 採購資通訊產品時，須請廠商說明其與大陸關聯性

資通訊產品定義

軟體

●資通軟體或系統，如應用軟體、系統軟體、客製化套裝軟體、APP及電腦作業系統等

硬體

●具連網能力、資料處理或控制功能者皆屬廣義之通訊設備，如個人電腦、可攜式設備及物連網設備等。

服務

●資通服務，如客服服務及軟硬體資產維護服務等。

重點注意事項

① 除大陸廠牌認定外，公務機關仍應視個案產品，檢視該產品是否屬**貼牌**或**核心組件**屬大陸廠牌之情形，並審慎評估處置以降低資安風險。

② 各機關辦理資通訊相關採購，得由各機關依個案特性及實際需要自行於採購文件中規定，是否**限制最終產品**(或連同所有零組件)**不得為大陸地區製造**。

③ 因業務需求且**無其他替代方案**，必須使用危害國家資通安全產品，應經機關資通安全長(下稱**資安長**)及上級機關資安長逐級**核可**後，由**函報數位發展部核定**。

④ 採購資通訊產品時，**請廠商說明**其與大陸**關聯性**(如公司持股、產品的生產/設計/製造)。

政府機關資安增能與職能培訓規劃

資安職能訓練 | **資安增能訓練**

資安長

約200人

法遵訓練時數低限	通識	專業
	3hr/年	無要求

- 資安長共識營
- 資安數位學習 (通識/線上課程)
- 中央及地方政府資通安全長會議

資安主管

約500人

法遵訓練時數低限	通識	專業
	3hr/年	無要求

- 資安主管治理研習
- 資安數位學習 (通識/線上課程)
- 職能訓練課程 (策略面為主)

資安專職人員

約1500人

法遵訓練時數低限	通識	專業
	無要求	12hr/年

- 資安人員專業訓練
- 政府資通安全巡迴研討會
- 資安數位學習 (專業/線上課程)
- 職能訓練訓練 (管理面、技術面為主)
- 稽核員訓練
- 資安技術工作坊
- 資安菁英人才培訓

資格要求
資安證照、證書各1張

113年政府機關資安人員專業訓練

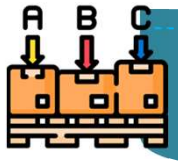
預計113年下半年開跑！

均有參訓機會

- 分批調訓A、B、C級資安專職人員
- 機關得保留一定人力

增加機關間聯繫

- 課程以團隊合作活動、分組研討為主
- 關係建立與專業知能並進



課程依面向分類

- 課程內容依制度面向分類
- 機關得依策略/管理/技術面向參與調訓

北中南東區辦理

- 為強化區域聯防，分北中南東部區域辦理
- 規劃一日課程，就近參與

113年新增高等三級考試「資通安全」類科

資安人才進用管道

- ✓ 考選部於112年12月28日公告113年起高考三級新增「資通安全」類科
- ✓ 至113年6月12日提報正額需用人數9名，報考人數199人

轉職系

各機關如有資安人力缺口：

- ◆ 建議循程序提報高考三級「資通安全」類科增額職缺
- ◆ 鼓勵機關非正式人員未來踴躍報考「資通安全」類科

零信任網路簡介

政府零信任網路架構：

參考NIST SP 800-207 零信任架構，包含3大核心機制

身分鑑別	• 多因子身分鑑別與鑑別聲明
設備鑑別	• 設備鑑別與設備健康管理
信任推斷	• 使用者情境信任推斷機制

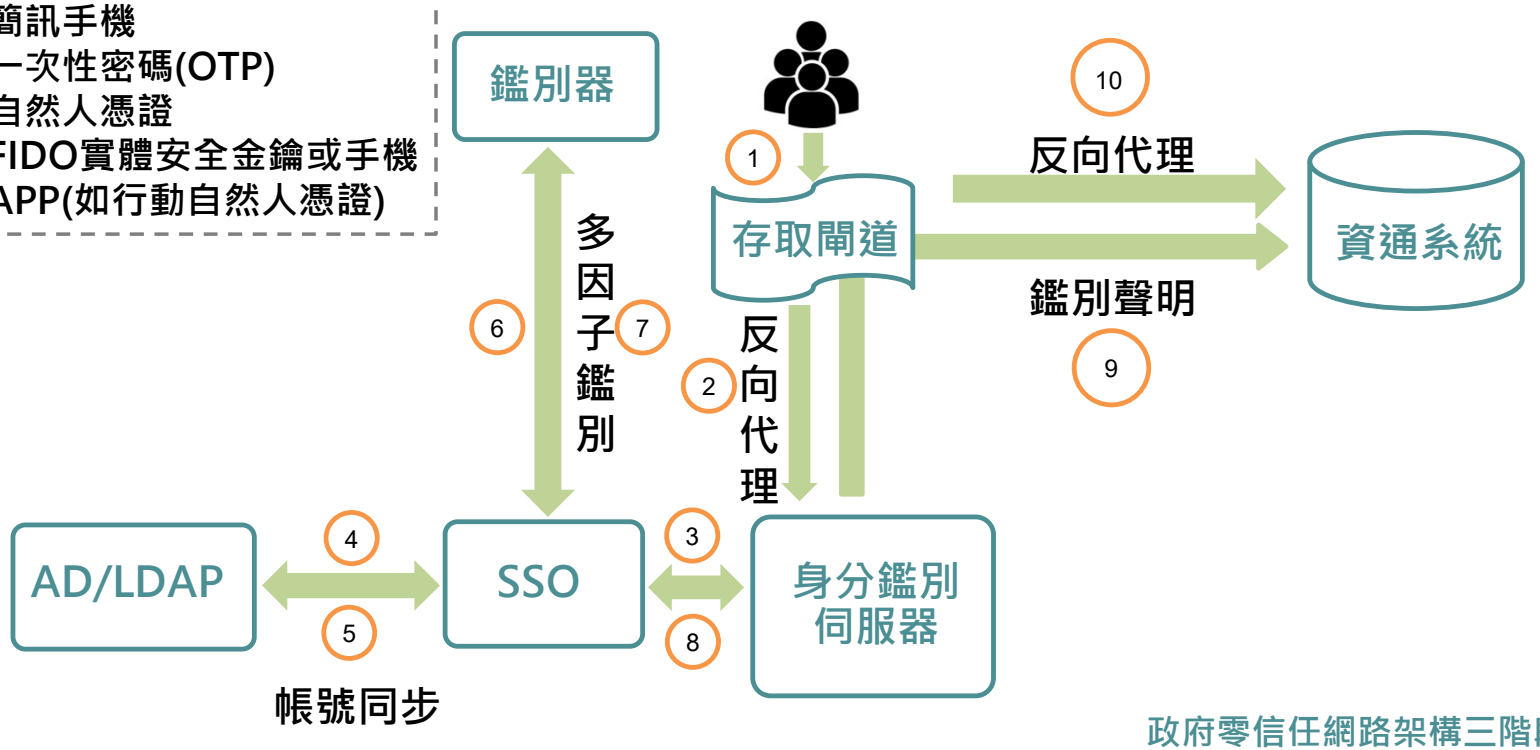
身分鑑別必要性防護項目

因應各機關現有資通系統環境基礎不同，提取零信任關鍵特性，訂定必要性防護項目

1	具備支援雙因子鑑別機制之身分鑑別伺服器，使資通系統解析鑑別聲明
2	身分鑑別伺服器可整合現有帳號身分認證
3	身分鑑別驗證通過須具有效期限（效期時間可依政策調控）
4	管理介面支援帳號新增、刪除及修改等功能與資通系統之管理設定
5	決策引擎針對任何存取依最小授權原則及鑑別結果允許或拒絕存取資通系統
6	登入(存取)行為均保存日誌紀錄，支援以時段與關鍵字為條件查詢
7	資通系統之存取一律走零信任架構並經過存取閘道管控
8	具備存取閘道實踐反向代理功能，依照決策引擎的判斷結果執行存取控制
9	零信任架構各組件間之通訊須加密（支援TLS1.2以上之加密協定）

零信任網路身分鑑別推動方式-以既有SSO為例

鑑別器類型：
- 簡訊手機
- 一次性密碼(OTP)
- 自然人憑證
- FIDO實體安全金鑰或手機APP(如行動自然人憑證)



政府零信任網路架構三階段：

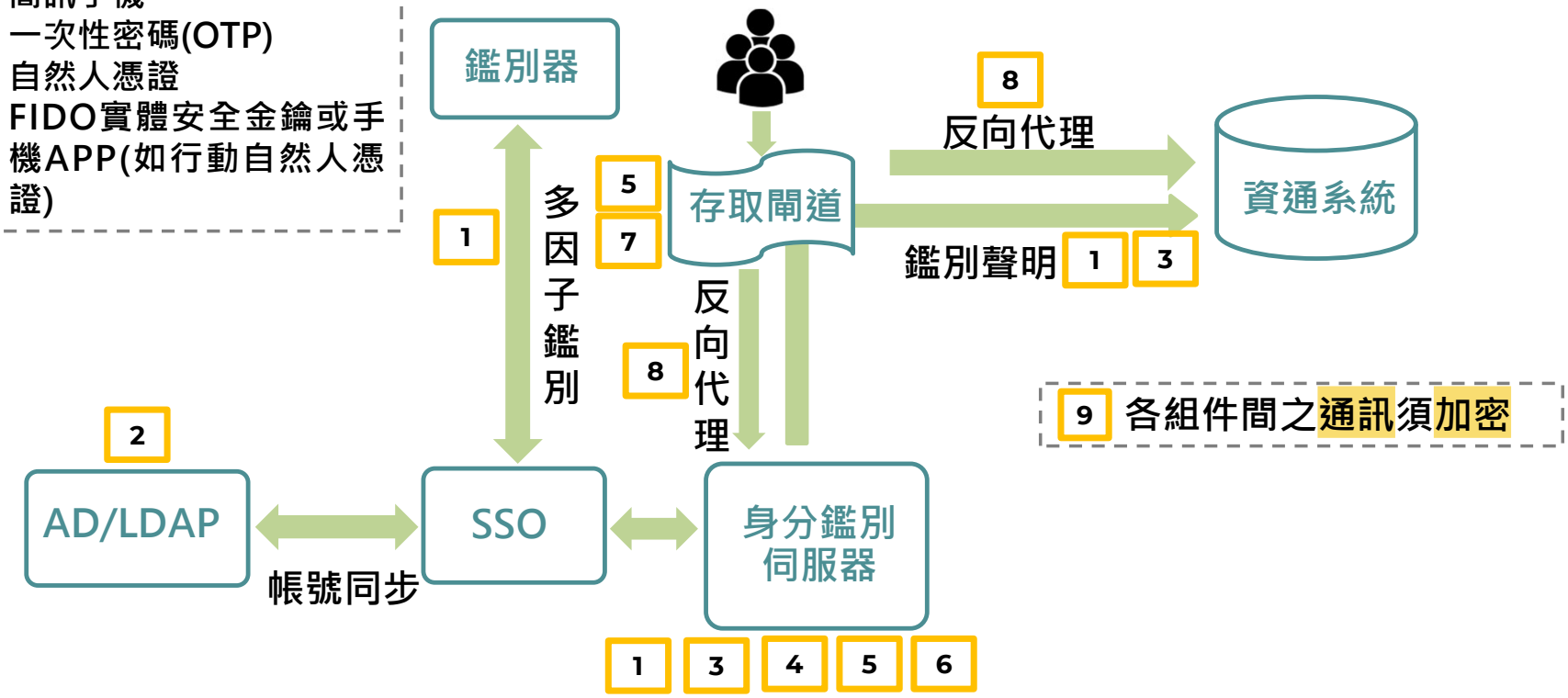
身分鑑別→設備鑑別→信任推斷

優先推動

零信任網路身分鑑別推動方式-以既有SSO為例

鑑別器類型：

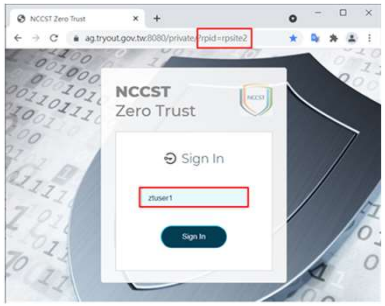
- 簡訊手機
- 一次性密碼(OTP)
- 自然人憑證
- FIDO實體安全金鑰或手機APP(如行動自然人憑證)



身分鑑別

以雙因子方式達成身分鑑別

- ✓ 運用如FIDO2相關技術鑑別使用者之身分



身分鑑別伺服器提供鑑別聲明(Token)

- ✓ 資通系統可解密並驗證鑑別聲明，並確保其機密性與完整性

鑑別聲明解析後範例

RP ID: [redacted]

User Name: [redacted]

Expire Time: 20[redacted]**T16:25:12+08:00[Asia/Taipei]**

Not Before: 20[redacted]T16:22:12+08:00[Asia/Taipei]

Issue At: 20[redacted]T16:22:12+08:00[Asia/Taipei]

身分鑑別功能符合性檢核(示例)

– 項次 2 整合現有帳號身分認證

功能說明	身分鑑別伺服器可整合現有帳號身分認證
實作說明	(1) 身分鑑別伺服器與身分提供者(IdP)、AD、LDAP 作帳號及身分驗證整合，資料同步至身分鑑別伺服器。例如：LDAP 帳號資料與 ZTA 身分鑑別資料同步 (2) 若有特殊網路架構之管理需求，而須建立 local 資料庫管理身分鑑別，應提供配套之帳號管理說明
驗證說明	(1) 測試若從 AD 將某帳號停用，是否有將相關帳號的狀態同步回身分鑑別伺服器管理平台，並確認無法存取資通系統 (2) 測試身分鑑別伺服器之管理帳號也透過 ZTA 身分鑑別登入身分鑑別伺服器之管理介面
佐證資料	(1) 與身分提供者之同步設定截圖、將某帳號從 AD 停用後確認無法存取資通系統之過程截圖 (2) 展示特權管理帳號透過 ZTA 身分鑑別登入身分鑑別伺服器管理平台之操作截圖
檢測結果	☐ 符合要求：符合檢測基準 ☐ 不符合要求：不符合檢測基準

– 項次 3 存取授權有效期

功能說明	身分鑑別驗證通過須具有效期限(效期時間可依政策調控)
實作說明	會談時間逾時(Session Timeout) 建議設定為 5-15 分鐘，可依機關資安政策設定
驗證說明	測試超過會談時間，系統會再發起身分鑑別要求
佐證資料	會談時間設定截圖、會談逾時後被登出之過程截圖
檢測結果	☐ 符合要求：符合檢測基準 ☐ 不符合要求：不符合檢測基準

項次2:主要檢核**身分鑑別伺服器**與現有身分驗證機制(AD、LDAP)**帳號是否同步**

項次3:主要檢核**會談時間逾時(Session Timeout)設定**

設備鑑別必要性防護項目

參考112年4月CISA發布零信任架構成熟度模型2.0訂定

1	設備具註冊管理機制，確保存取資源的請求者為合法設備
2	設備存取資源時須經過存取權限控管
3	設備鑑別伺服器提供管理介面，可實現設備管控追蹤，並可查詢設備清單及日誌
4	設備鑑別伺服器提供整合介面供其他組件使用

肆、資安稽核及網路攻防演練常見發現

資安稽核常見缺失

① 盤點完整性不足 資通系統及資訊

常見樣態

- **僅列核心系統**
- 支持核心業務列為**非核心系統**
- **設備**未盤點
- **IoT/OT系統**未盤點

案例

• 維護計畫(細則§6)

機關核心業務
- Aa作業
- Bb服務

支持核心業務之系統

• 資訊資產盤點結果

系統名稱	分級	核心系統
Aa作業管理系統	普	否
員工入口網		
官方網站		

機關其他資通系統未納入

• 設備未納入盤點

設備未盤點納入清單

解決方式

- 盤點範圍應為**全機關**。
- **不**應**侷限於資訊單位**或連網**設備**(有線/無線)。
- 包含**工控系統**(ICS)或**運營科技**(OT)系統及相關**設備**。

資安稽核常見缺失

② 與備援機制業務持續計畫

常見樣態

- **缺乏業務單位的參與**
- 未演練**備援機制**之**有效性**。

案例

- 僅**演練備份作業**，未測試備份或備援**有效性**。
- 演練時，僅資訊人員辦理，應將**相關人員納入**(作業人員、委外廠商)。

解決方式

- 依實際**業務需求**與**業務單位**共同評估、演練及精進BCP
- 以**業務持續運作演練**檢視**備援機制**，並納入**業務單位**共同執行

資安稽核常見缺失

③ 機制待改善
內部稽核

常見樣態

- **侷限於資訊單位**
- 各**內部單位輪流受稽**方式辦理
- **稽核自身所管業務**之情形

案例

機關設有ABCDE內部單位

- **稽核小組：**B、C成員擔任

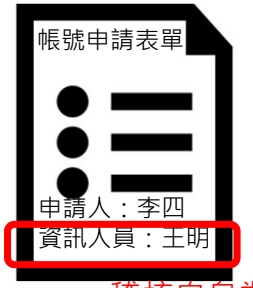
僅納入機關部分成員(資訊室、政風室)

- **稽核範圍：**

111年：A、C、D
112年：B、F

輪流受稽

- 稽核人員：王明



稽核自身業務
球員兼裁判

解決方式

- 範圍為**全機關**
- 成員涵蓋**各單位**
- 追蹤**改善機制**

資安稽核常見缺失

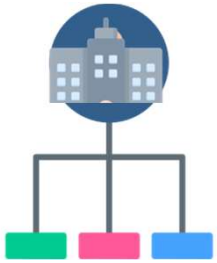
④

資安稽核對所屬或所管

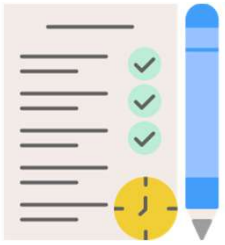
常見樣態

- **非由中央目的事業主管或上級機關名義辦理**
- 稽核小組**員額偏少**
- **稽核形式**與機關規定**不符**

案例



A機關下設3個局處



機關自訂稽核作業辦法

稽核小組：最少7人，並由機關、專家學者、XXX擔任。
稽核方式：實地稽核。
⋮ ⋮

應以A名義提出稽核報告

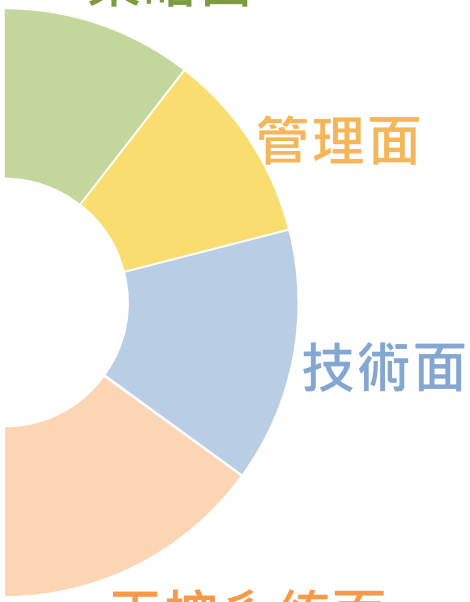
稽核委員人數不足

稽核方式錯誤

解決方式

- 應由**機關名義**提出**稽核報告**
- 配置**足額之稽核委員**，並採**合規之稽核方式**辦理

113年行政院資通安全稽核重點項目



(註：關鍵基礎設施提供者新增稽核面向)

113年稽核重點項目

一、**資安治理成熟度**評估及因應作為 自評方式適切性 結果確認方式 未達目標之策進方式

二、資安責任等級分級辦法應辦事項-**認知與訓練**符合情形 全機關 專業課程 證照有效性

三、禁止使用**危害國家資通安全產品**及其**管控措施** 作法 盤點及列冊 管控措施 委外要求

四、自行、**委外**開發**資通系統**之**盤點及定期更新**情形 標示外部元件 軟體物料清單

五、**VANS導入**及因應情形 導入範圍 每月上傳 高風險弱點之緩解措施及管理作為

六、資安事件**通報、應處**、結報、審核等**法遵事項**逾時之改善 逾時改善作為 熟悉程序

七、個資外洩**資安事件處理**情形 因應措施 個資外洩影響程度 通知當事人

八、受稽機關資安事件駭侵**根因調查**情形 根因調查 跡證保存

九、**營運持續**計畫 OT系統納入 備援及備份

十、**ICS(OT)網路架構** 網路架構 邊界防護 定期檢視

十一、**實體**與環境**防護** 存取授權 實體隔離機制 實體防護 廠商/陪同者管控作為

網路攻防演練常見發現

- 針對主要弱點類型列出**3項**常見發現事項樣態及案例

未落實通行碼強度檢查機制

注入漏洞

帳號密碼外洩

未落實通行碼強度檢查機制

機關未強化通行碼設定原則

通行碼之提示內容遭暴力破解

樣態&案例

檢測方式&改善建議

開發者

- ✓ 符合通行碼複雜度原則
- ✓ 設定密碼歷程紀錄等管控機制
- ✓ 登入頁面使用圖形驗證碼等機制

使用者

- ✓ 避免使用公開易取得資訊(ex.廠商統編、學校代碼等)
- ✓ 避免字元過短與簡單英數組合

注入漏洞

樣態&案例

網站未妥善處理輸入內容，可輸入惡意指令並當成SQL語句執行

使用者內容以黑名單形式過濾，但過濾字串未周全，導致攻擊者以特定形式繞過

檢測方式&改善建議

開發者

- ✓ 對使用者輸入內容進行嚴格過濾，或採用白名單機制過濾輸入內容
- ✓ 改以參數化形式傳值，避免SQL語句被竄改或截斷

帳號密碼外洩

密碼以明文方式或以不安全編碼方式進行儲存

將帳號密碼寫入網頁原始碼等易遭外部使用者取得之位置

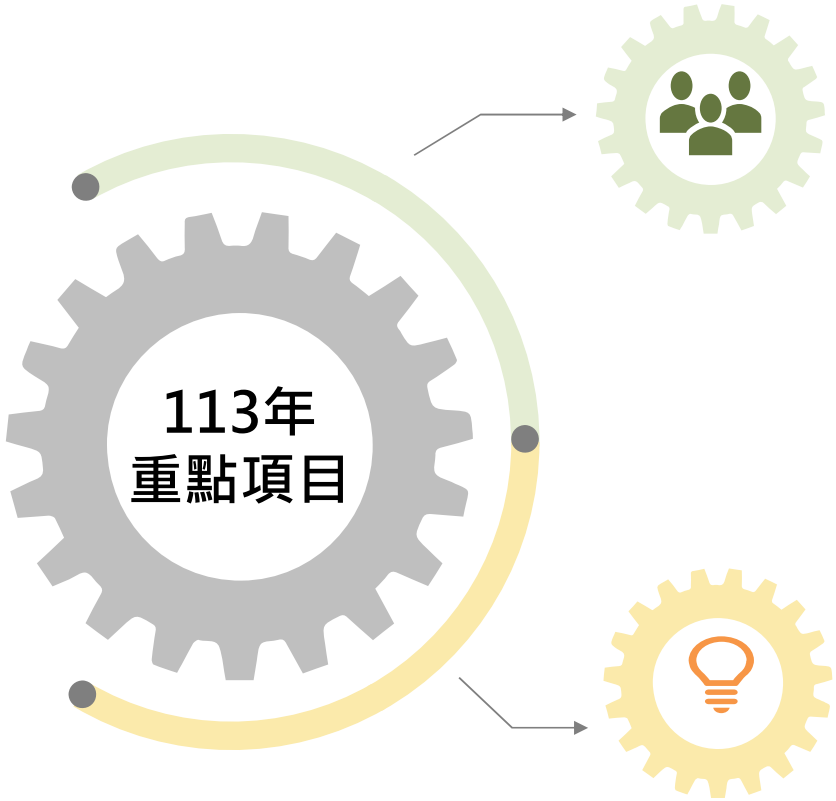
樣態&案例

檢測方式&改善建議

開發者

- ✓ 所有檢查應於伺服器端進行，僅回傳必要之檢查結果，避免將機敏資訊放入網頁回應封包當中
- ✓ 程式開發完成應重新檢視網頁原始碼內容，避免將機敏資訊放於網頁原始碼之註解當中

113年網路攻防演練重點項目



實兵演練擴大演練機關

- 除A級機關與地方政府B級機關，將擇定4週演練時間(**不預先通知演練時間**)，開放**GSN網段內全國公務機關**對外服務系統為演練目標

加強資安事件等級認知

- **通報等級錯誤**，經勸導未進行修正者，納入**加重扣分**
  - ✓ 案例：演練時取得某機關一般個資資訊，機關認定演練非真實事件，則通報2級資安事件，經勸導後未於24小時內修正，將額外扣分

數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理