資通安全業務重點工作

數位發展部資通安全署
112年11月

大綱

數位發展部資通安全署
Administration for Cyber Security, moda

1. 法遵事項推動辦理情形

2. 重點工作宣導

3. 近期政府機關資安事件案例分享及防護建議

1.法遵事項推動辦理情形

1.1資安責任等級核定情形

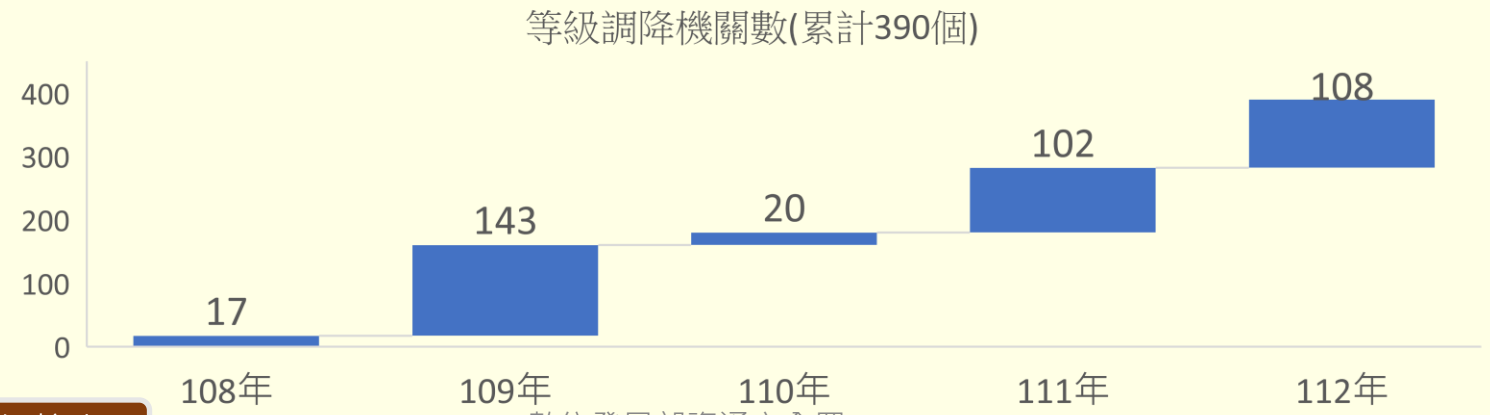
112年度各機關資安責任等級核定

法遵事項

- 依資通安全責任等級分級辦法第3條規定，各機關每2年需報主管機關重新核定(備)責任等級，已於112年7至9月間陸續核定(備)，資安責任等級異動情形如下(**統計至112年9月30日**)：

	A級	B級	C級	D級	E級	總計
中央機關	49	111	452	234	114	960
地方政府	0	110	551	4,940	738	6,339
特定非公務機關	44	103	93	83	27	350
合計	93	324	1,096	5,257	879	7,649

(相較112年2月份，納管對象由7720個機關變更為7,649個機關)

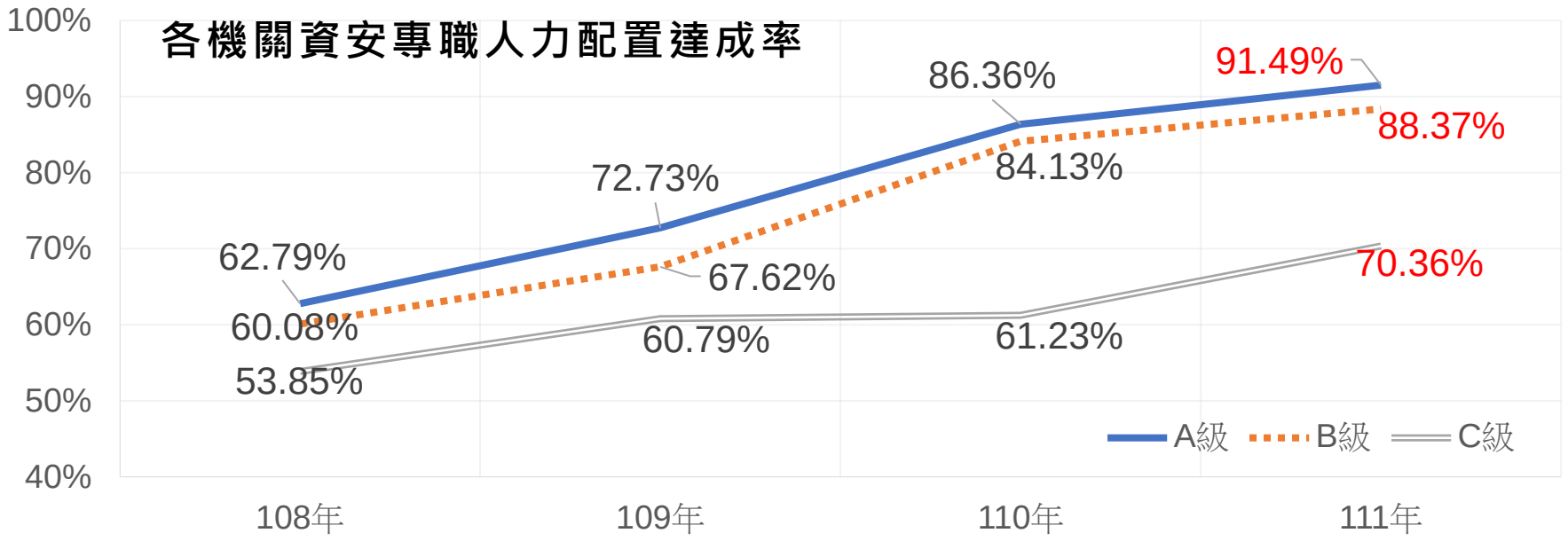


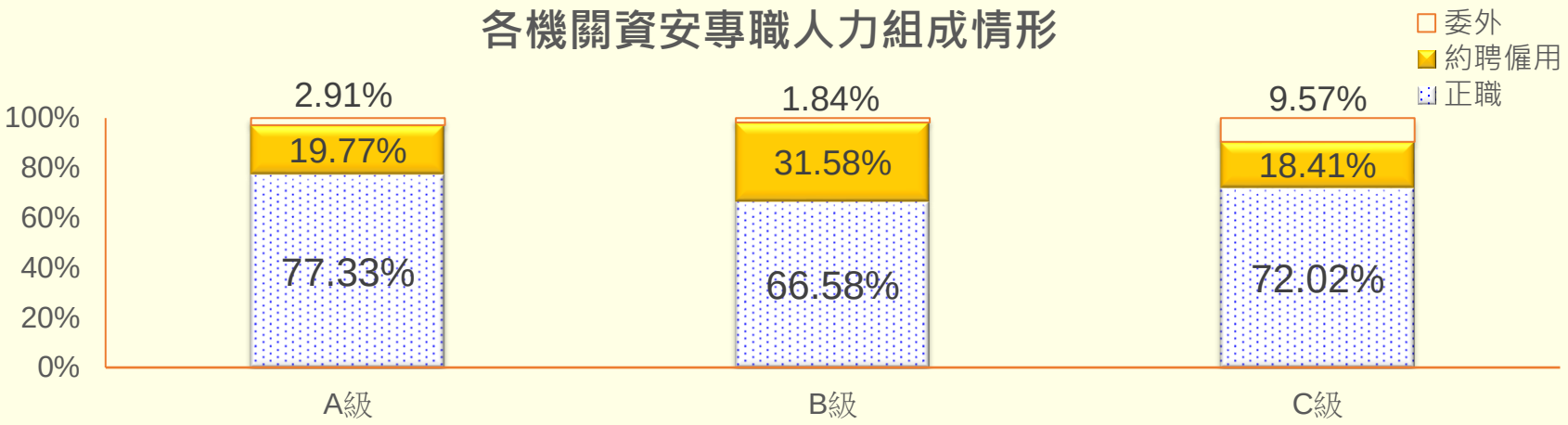
1.法遵事項推動辦理情形

1.2實施情形概況

各機關資安人力配置情形

法遵事項





資訊資產設備盤點情形

法遵事項

- 因應近期各式資通設備之資安威脅加劇，爰依資通安全法施行細則第6條規定，爰111年實施情形資料中，增列提報「**機關資通訊設備清冊**」
- 提報範圍建議參照行政院**主計總處「財物標準分類」**之財物編號，盤點**全機關資通訊設備**，至少包含
  - 「機械及設備分類明細表」項下之「電腦系統」(分類編號3140101~3140503)各類財產
  - 其他非屬前開項下之資通設備：
    例如：遙控無人機(分類編號4030204-06)、手機(分類編號4050202-05)等資通設備亦請納入盤點

資訊資產設備盤點情形

法遵事項

附表3-3-資通訊設備清冊

#	設備名稱	廠牌名稱	數量	備註
1	手機	Apple iPhone 11	-	司
2	手機	Apple iPhone 11 Pro.	1	司
3	手機	ASUS ZenFone 2	1	司
4	手機	SAMSUNG A13 5G	47	司
5	可攜式無線路由器	D-LINK DWR-933	8	部
6	光纖通道交換器	HPE 8/8 Base 8-port Enabled SAN Switch	1	部
7	光纖通道交換器	HPE 8/8 SAN Switch		

管理單位

應包含廠牌資訊及型號

常見錯誤態樣

- 僅有設備名稱，未有廠牌資訊或型號
- 僅盤點資訊單位所管理資產
- 未包含IOT設備

各機關應辦事項辦理情形

法遵事項

前三未達成項目		
責任等級	應辦事項工項	未達成機關比例
A級	1.資通系統分級及防護基準 **2.資安職能訓練證書** 3.政府組態基準	10.64% 10.64% 8.51%
B級	1.端點偵測及應變機制 **2.資安職能訓練證書** 3.資通安全專職人員配置	9.30% 8.84% 8.37%
C級	**1.資安職能訓練證書** 2.資安專業證照 3.資通安全弱點通報機制	23.73% 22.69% 20.93%

1. 部分系統未有符合防護基準或部分仍未導入GCB之情形，請規劃改善並於未改善前**擬具管理作為**、**加強監控**，降低資安風險
2. 依規定112.8.23前**C級**機關應**導入VANS**、**B級**以上公務機關應**導入EDR**

推展資安職能訓練

數位發展部資通安全署
Administration for Cyber Security, moda

- **擴增核心職能訓練課程開班數及評量**
  - 112年專案增開15班「資通安全概論」全額補助班(10月至12月)**目前已報名額滿。**
    - ✓ 「資通安全責任等級A、B、C級」公務機關同仁（地方機關優先錄取）
  - 112年11月至113年2月**增開**資安職能訓練**評量場次**，請至國家資通安全研究院「資安人才培訓服務網-最新消息」查詢（網址：https://ctts.nics.nat.gov.tw/）。

112年專案補助班開設之訓練機構		
北部	中國文化大學	台北市大安區建國南路二段231號2樓
中部	國立中興大學	台中市南區興大路145號
南部	崑山科技大學	台南市永康區崑大路195號

資通安全專業證照宣導

數位發展部資通安全署
Administration for Cyber Security, moda

資通安全專業證照清單

日期：112 年 2 月 14 日修正

序	發證機構(單位)	管理類(19)	技術類(92)
1.	已簽署國際認證論壇(International Accreditation Forum, IAF)多邊相互承認協議(ISO/IEC 27006 範圍)之認證機構所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構[1]	1. ISO/IEC 27001:2013 Information Security Management System(ISMS) Auditor/ Lead Auditor (請於 114 年 10 月 31 日前完成轉版) 2. ISO 22301 Business Continuity Management System(BCMS) Auditor/Lead Auditor 3. ISO/IEC 29100 Lead Privacy Implementer Information technology — Security techniques — Privacy framework (111 年 3 月 15 日停止認定) 4. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor 5. ISO/IEC 27001:2022 Information Security Management System(ISMS) Auditor/ Lead Auditor Lead Auditor 相關證照應具有效性，除提出證照外，尚須提供當年度至少有 2 次實際參與該證照內容有關之稽核經驗證明。	

ISO/IEC 27001:2013 資通安全專業證照認列至 114年 10 月 31 日止，請於該期限前完成轉版。

- **資通安全專業證照取得方式:**

可洽各資通安全專業證照之相關培訓機構（單位）諮詢。

- **資通安全專業證照清單內容:**

請至本署「資安法規專區」之「資通安全專業證照清單」網頁中下載電子檔。

請各機關應依資通安全管理法相關規定，自行編列適當預算因應。

1.法遵事項推動辦理情形

1.3VANS推動情形

VANS推動情形

法遵事項

依「資通安全責任等級分級辦法」第11條及附表應辦事項規定，資通安全責任等級C級之公務機關應於112年8月23日前完成VANS上傳作業。

A級機關
導入期限111/08/23

- A級之公務機關
- A級之CI提供者

導入率 100%

B級機關
導入期限111/08/23

- B級之公務機關
- B級之CI提供者

導入率 100%

C級機關
導入期限112/08/23

- C級公務機關
- 無C級CI提供者

導入率 99%

1.統計截止日：112年10月30日
2.VANS之申請表單、教育訓練教材(含數位課程)及常見問題FAQ，詳見：
https://www.nics.nat.gov.tw/Vans.htm?lang=zh

VANS導入作業常見問題

法遵事項

機關執行上傳步驟時，未檢視資產盤點資料是否成功提交

- 上傳前，應檢視資產盤點資料的欄位順序或格式正確性 (與範本一致)
- 上傳後：
  - 建議查詢VANS系統「機關資產資訊」功能項下的「資通系統資產列表」及「使用者電腦資產列表」，確認資料是否成功匯入
  - 確認已收到VANS系統自動發送的電子郵件通知 (需啟用設定，系統將回傳弱點比對通知或上傳解析失敗)

資通系統的操作步驟相同！

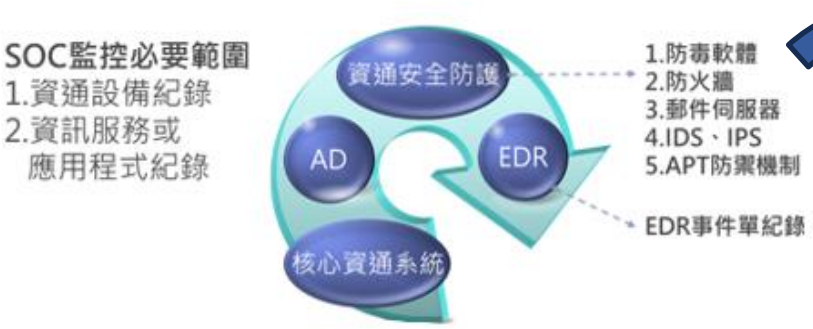
1.法遵事項推動辦理情形

1.4資通安全威脅偵測管理機制

資通安全威脅偵測管理機制

法遵事項

- **建置威脅偵測機制，確保防護目標與對應防護項目納入資安監控範圍**
  - A、B級公務機關SOC之監控範圍除原有之資通安全防護項目，並應擴充「端點偵測及應變機制」、「目錄服務系統(AD)」及「核心資通系統」日誌之情資收容能力。
  - 本署每月綜整分析SOC監控資料，產製資安聯防監控月報於通報應變網站供機關下載參考運用。



SOC監控範圍

辦理項目	辦理內容	資安責任等級				
		A	B	C	D	E
資通安全防護 (啟用，並持續使用及適時進行軟硬體之必要更新或升級)	防毒軟體 網路防火牆 電子郵件過濾機制	★	★	★	★	
	入侵偵測及防禦機制 應用程式防火牆	★	★			
	進階持續性威脅攻擊防禦措施	★				

資通安全防護項目

A、B級公務機關SOC回傳作業應辦事項

法遵事項

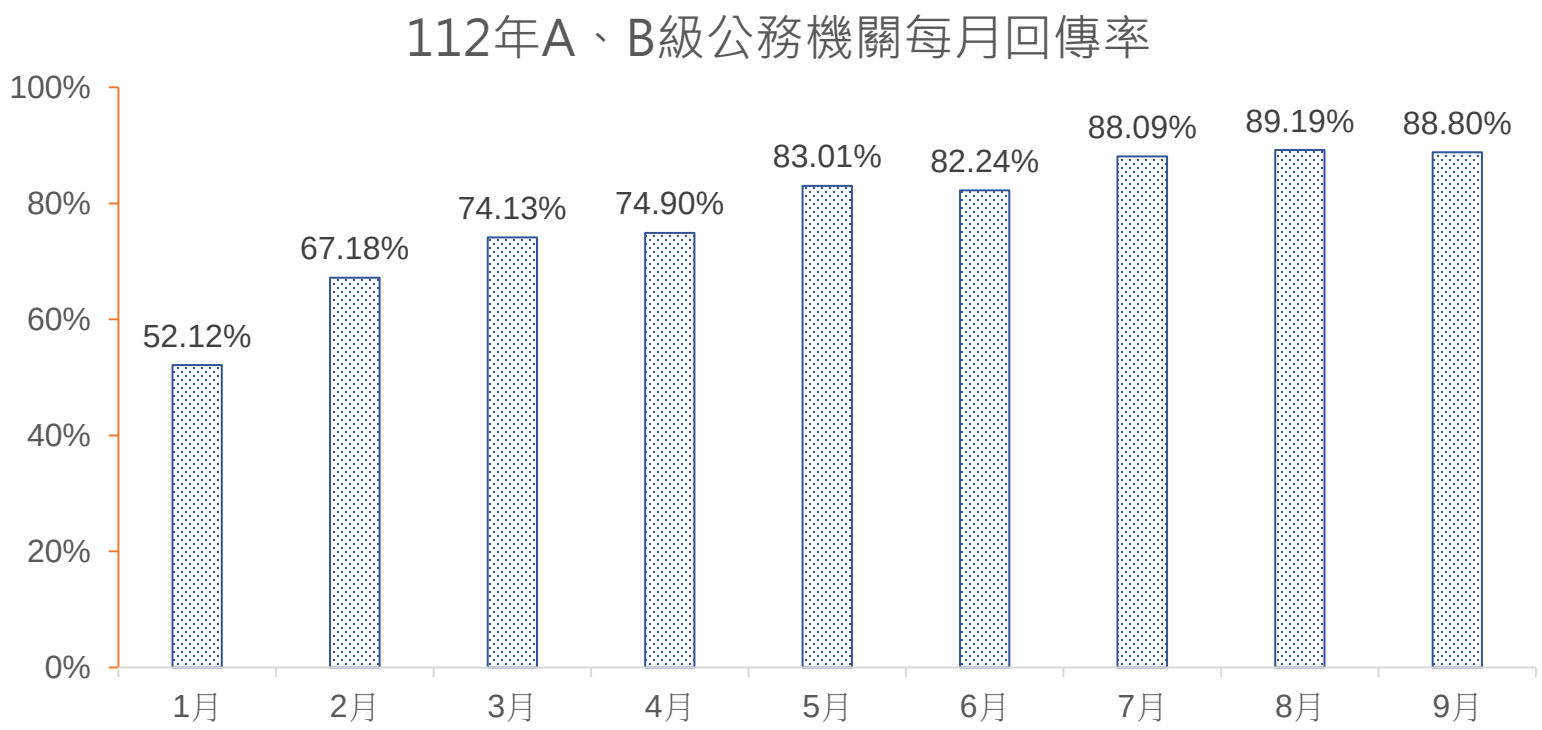
- SOC機制不論自行或委外監控，請A、B級公務機關注意以下重點，並**每月掌握回傳情形**
  - 在系統觸發並記錄事件資料時，應回傳「資安監控單」，並確認可明確辨識之威脅種類，非僅回傳「其他」類之情資
  - 每月5日前回傳「監控設備狀況單」，並確實填寫資安防護類型
  - 為利各機關檢視，本署已規劃改版資通安全作業管考系統之「資安監控作業」，提供各機關查詢自身及所屬機關SOC回傳情況

檔案格式	STIX 2.1
威脅種類	入侵攻擊、惡意內容、惡意程式、資訊蒐集、入侵嘗試、服務阻斷、資訊內容安全、詐欺攻擊、系統弱點、其他
資安防護類型	資通安全防護項目、EDR、AD及「核心資通系統」日誌

A、B級公務機關SOC執行現況

法遵事項

- 多數機關已完成SOC資料回傳作業，其中16個機關尚無回傳資料，後續將發函請該些機關確認執行情形。



1.法遵事項推動辦理情形

1.5端點偵測(EDR)資安防護機制

端點偵測(EDR)資安防護機制說明

法遵事項

01

依據法遵要求

A、B級公務機關應辦事項：於初次受核定或等級變更後之二年內，完成端點偵測機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。

02

導入目標

應以全機關導入為目標，若因經費預算問題，可依系統重要性逐步完成導入作業，並擇選通過資安院連通測試之EDR廠牌(公告於資安院網站EDR專區)。

03

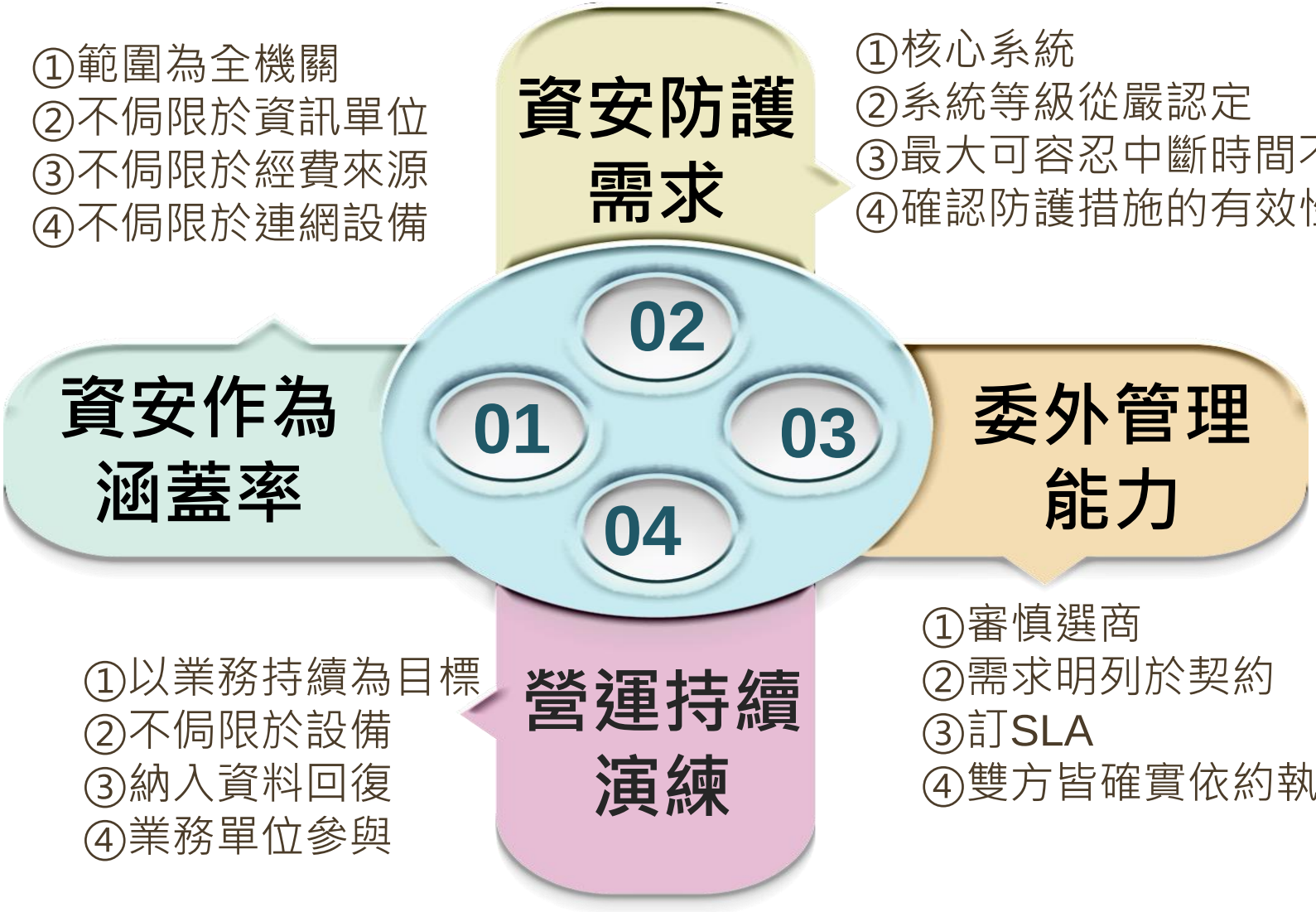
提交資料方式

經EDR端點掃描告警資訊並分析確認為資安事件後，產出事件資訊，透由機關SOC機制上傳，機關亦可查看回傳之「監控設備狀況單」是否含EDR設備，確認上傳機制正常運作。

2.重點工作宣導

2.1資安稽核常見發現

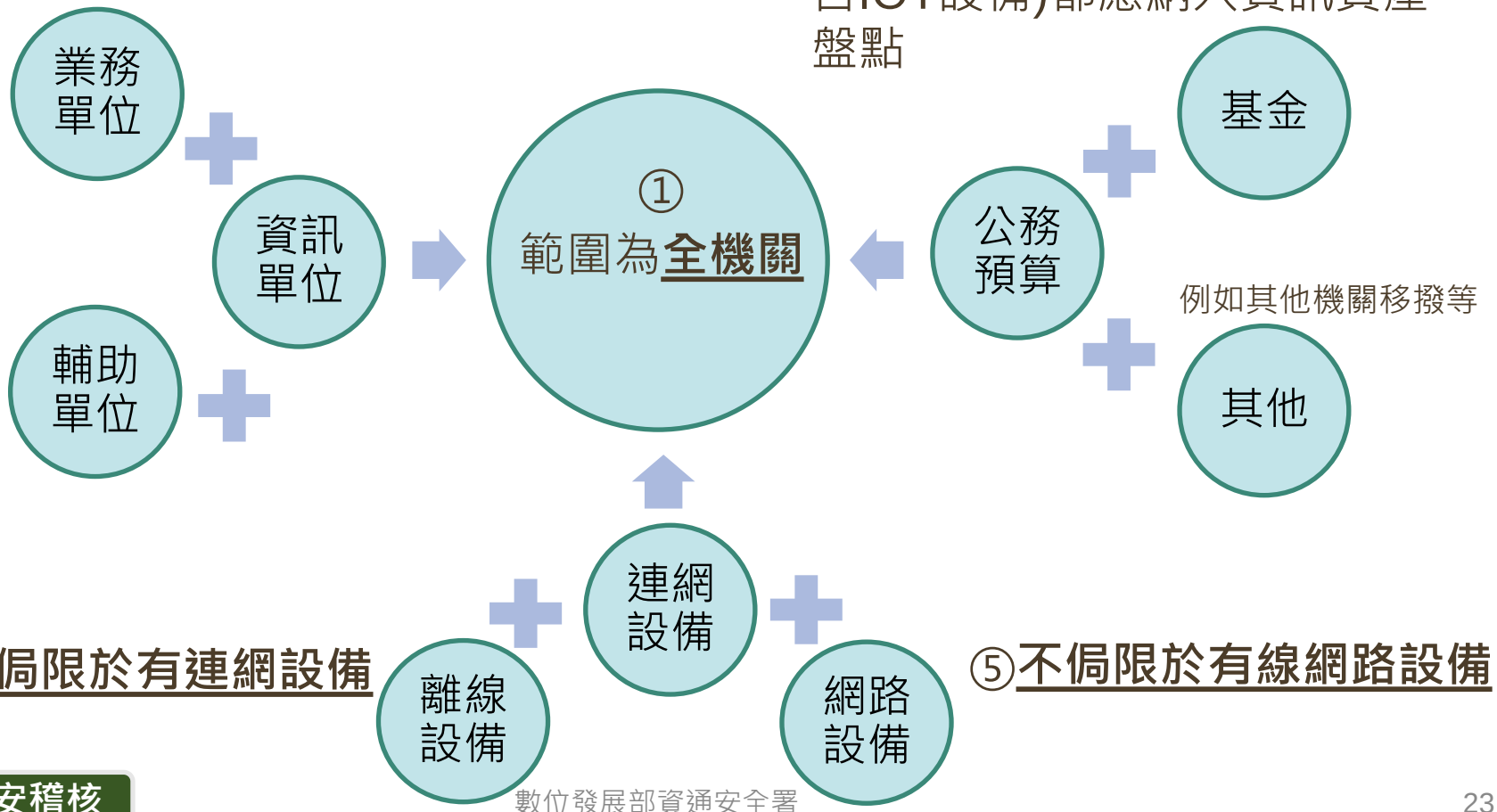
資安稽核共通性發現及建議作為



資安作為涵蓋率應為全機關

②**不侷限於資訊單位**
所有機關內的單位，不論正式編制或任務編組皆應納入

③**不侷限於取得之經費來源**
只要在機關內有使用到的(包含IOT設備)都應納入資訊資產盤點



④**不侷限於有連網設備**

⑤**不侷限於有線網路設備**

核心系統認定及防護措施有效性

明確定義核心系統

防護需求從嚴認定

①**核心系統**等級應**從嚴**、**從實**、**從難**認定
②核心系統最大可容忍中斷時間不宜過長

確認防護措施有效

①實施安全性檢測，透過**複測**確認修補有效
②透過**演練**確認**防護措施**可阻擋或緩解攻擊
③確認**相關文件**資訊及要求**一致**，並由適當層級主管核定確認

強化委外管理能力

選好商

1. 資通系統**籌獲前評估**資通系統**防護需求等級**
2. 訂定合理之**資安要求**及**資訊服務等級協議(SLA)**，並載明於**招標文件及契約**
3. 將委託案相關**資安作為**納為**評選項目**，要求廠商說明
4. **評選委員**應包含至少一位**資安專業人員**

管好商

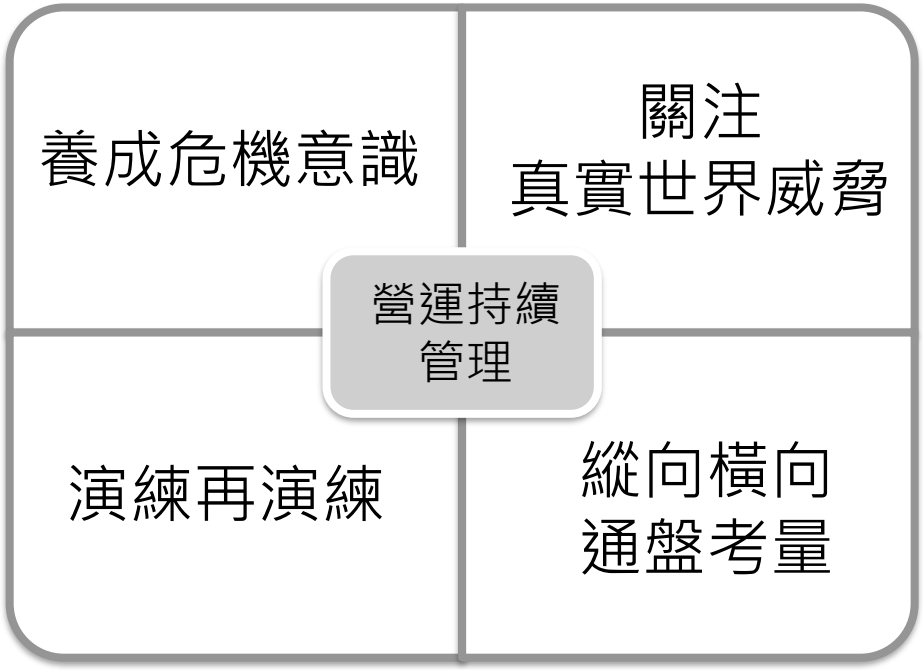
1. 落實情形由**管理及需求單位一線監督**及確認，**資通安全專職人員二線協助**勾稽確認
2. 以**適當方式**定期或不定期辦理受託者**資安稽核**
3. 將**資安事件**之**通報及應處納入資訊服務等級協議(SLA) 項目**

參考「資通系統籌獲各階段資安強化措施」https://acs.gov.tw/laws/guide/rules-guidelines/1355
及行政院公共工程委員會112年09月25日資訊服務採購作業指引

營運持續全面管理

考量
系統和資料
①備份、備援
②同地、異地

組成
完整演練對象
①資訊單位
②業務單位
③支援單位



設計
複合式全災害情境
①天然、人為、資安
②從嚴、從難、從實

建立
緊急應變指揮架構
①向上通報對象
②橫向連結對象
③協處的支援單位

演練後才是精進的開始

實際認知到不足的面向，調整後反覆練習

工程會「資訊服務採購契約範本」

- **契約內容應明確敘明廠商權責，可參考公共工程委員會「資訊服務採購契約範本」。**
  - 工程會官網-招標相關文件及表格：https://www.pcc.gov.tw/cp.aspx?n=99E24DAAC84279E4

- **機關仍應針對委託業務調整契約範本，依需求適當增減契約內容。**
  - 不應直接以契約範本之要求全數要求廠商，應依委託項目及機關需求增減契約內容，明確甲乙雙方責任

2.重點工作宣導

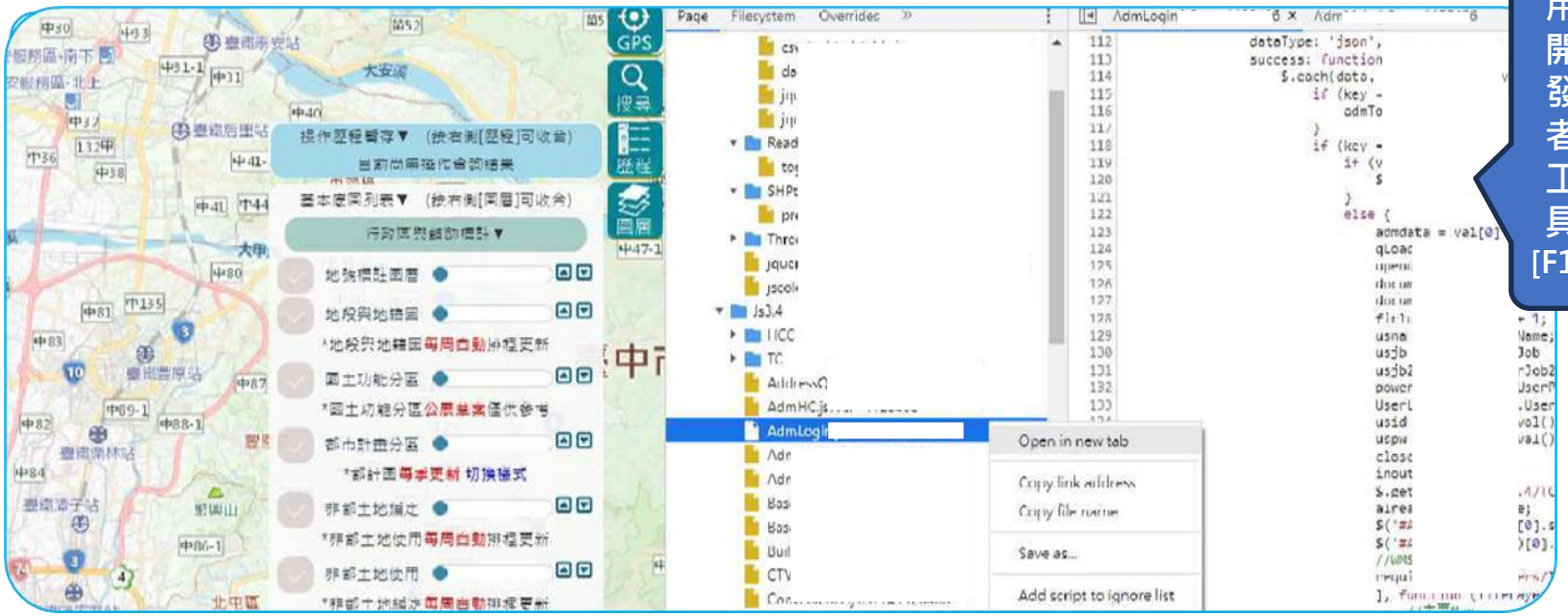
2.2實兵演練重點與常見發現

認證及驗證機制失效

- **多個縣市政府圖書館系統**
  - 網站揭露密碼規則，如生日4碼
  - 密碼僅數字4碼，暴力破解，成功登入可取得讀者個資。
  - 並可橫向連結至圖書相關系統，如便民借還系統、自動化管理系統、閱讀網站等。
  - 建議機關提高密碼強度（複雜度、字元數）

加密機制失效

- 地理資訊系統、資訊平台、行政管理平台：
  網頁原始碼揭露可使用之帳號、密碼



案例1

```
        //#region
    });

    // //#region
    // $('#icon').click(function(e){
    //     $('#account').val('superuser');
    //     $('#password').val('pwd@1234');
    //     $('#code').val(code);
    //     $('.btn-send').click();
    // });
    // //#endregion
```

案例2

```
            queryTask.execute(query).then(function (results) { towngra = results })
        })
    })
    if (location.href.indexOf('ain=a') !== -1) {
        $.ajax({
            type: "POST",
            url: "../Api/users/login",
            data: {
                帳號: 'admin1234',
                密碼: 'admin5678',
            },
            success: function (data) {
                if (data.status) {
                    landtoken = data.token
                    $('#userName').html('<img src=
                    $('#toolList').html(
```

DDoS演練

- 演練參照DDOS歷史攻擊事件，本次演練攻擊時間設計20-40分鐘之間，以檢視機關相關防禦機制。

演練方式：
- **網路層攻擊：消耗目標網路頻寬，使其無法正常使用。**
- **應用層攻擊：佔盡目標服務連線數量，使其無法正常使用。**

演練單位	演練標的	演練規格	標的狀態	演練結果
A	機關Domain	應用層攻擊	成功防禦攻擊，無影響可用性	防禦成功
B	DNS伺服器	網路層攻擊	攻擊持續至第30分鐘時，DNS服務中斷。	攻擊成功

- 建議機關重新檢視DNS伺服器防護機制，評估強化服務頻寬或縮短流量清洗反應時間等，以提升系統對與DDoS攻擊之抵禦能力。

2.重點工作宣導

2.3資安法修法草案重點

資安法修法重點-修法期程

資安署 112年10-11月

8/17 - 9/25
修法工作坊

9/22
草案預告

10/17 - 11/16
修法說明會及法制教育訓練

數位部→行政院 112年11-12月

11/20
預告期滿

11月底
綜整意見

12月
函送行政院

資安法修法重點-主管機關調適

- 核定國家資通安全發展方案§4
- 設置國家資通安全會報§5
- 核定關鍵基礎設施提供者§19

行政院
【決策】

- 本法主管機關§2Ⅰ
- 國家資通安全會報決議事項之管考及績效評核§5
- 規劃推動國家資安政策等相關事宜§6
- 授權子法之訂定發布§7Ⅲ、8Ⅳ、9Ⅱ、15Ⅱ、17Ⅳ、18Ⅲ、24Ⅳ、26Ⅱ、32
- 接受查詢危害國家資通安全產品清單及廠商§11

數位發展部
【規劃】

- 辦理國家資安業務§2Ⅱ
- 核定或備查資安責任等級§7
- 稽核資安維護計畫實施情形§8
- 建立情資分享機制§9
- 接受稽核報告§16、20、21
- 接受資安事件通報§17
- 統籌公務機關資安人力§18
- 特非機關重大資安事件之協助§24

資通安全署
【規劃與執行】

公務機關

- 收受及稽核所屬、所轄、所監督公務機關之實施情形§14~16
- 接受資安事件通報、改善報告、重大資安事件協助及公告§17

【執行】

中央目的事業主管機關

- 指定關鍵基礎設施提供者§19
- 監管所管之特非機關§20~22
- 特非機關重大資安事件協助§24
- 行政調查§25
- 裁罰特非機關§27~29

2.重點工作宣導
2.4資安人才培育政策

政府資安跨域人才培育規劃

規劃轉任資訊處理職系(資安人員)訓練制度

- 依現職公務人員調任辦法規定，公務人員具有擬任職務法定任用資格人員，得於不同職務間調動，如：一般行政職系轉任資訊處理職系(資安人員)。
- 本署於112年規劃360小時(或20學分)符合轉任之相關課程，未來提供有需求機關同仁參用。

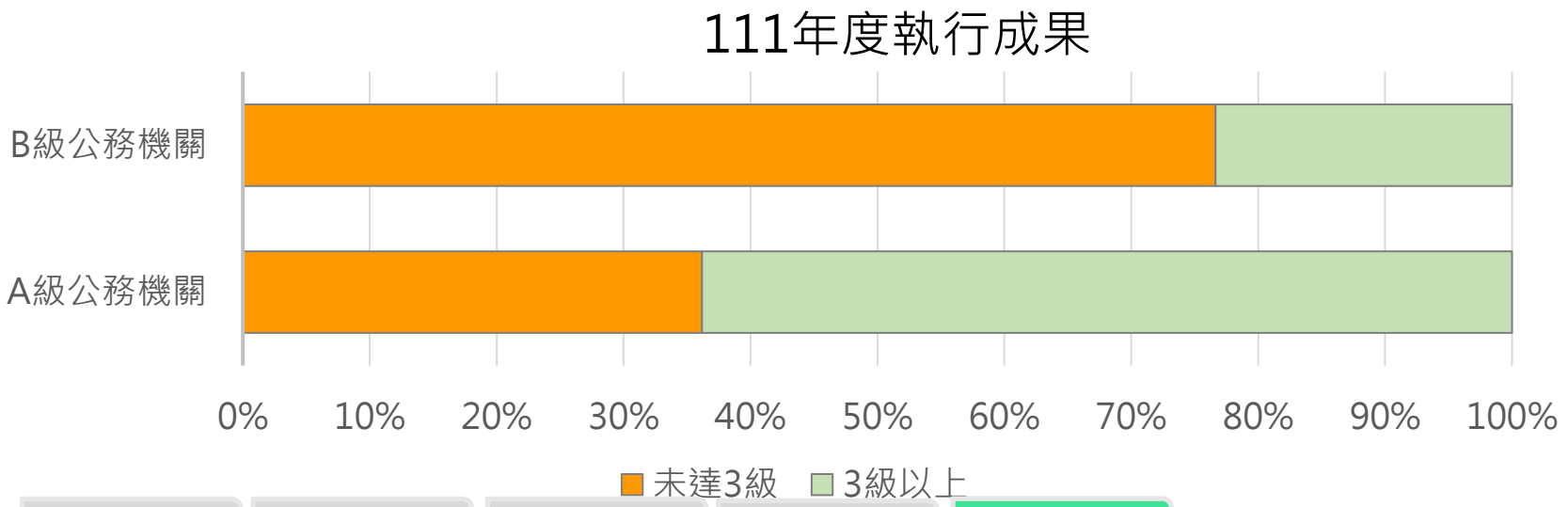
公務人員考試增設資安類科推動

- 經與考試院跨院協調，規劃於公務人員高等考試三級考試**增設資通安全類科**，增加政府機關徵才管道。
- 本署業與利害關係人多次會議討論後，其應試專業科目前暫時規劃4門。
- 本署業已協助研具應考資格、考試方式及應試科目之**說明報告**，已函主管機關請辦後續相關事宜。

2.重點工作宣導
2.5資安治理成熟度推動

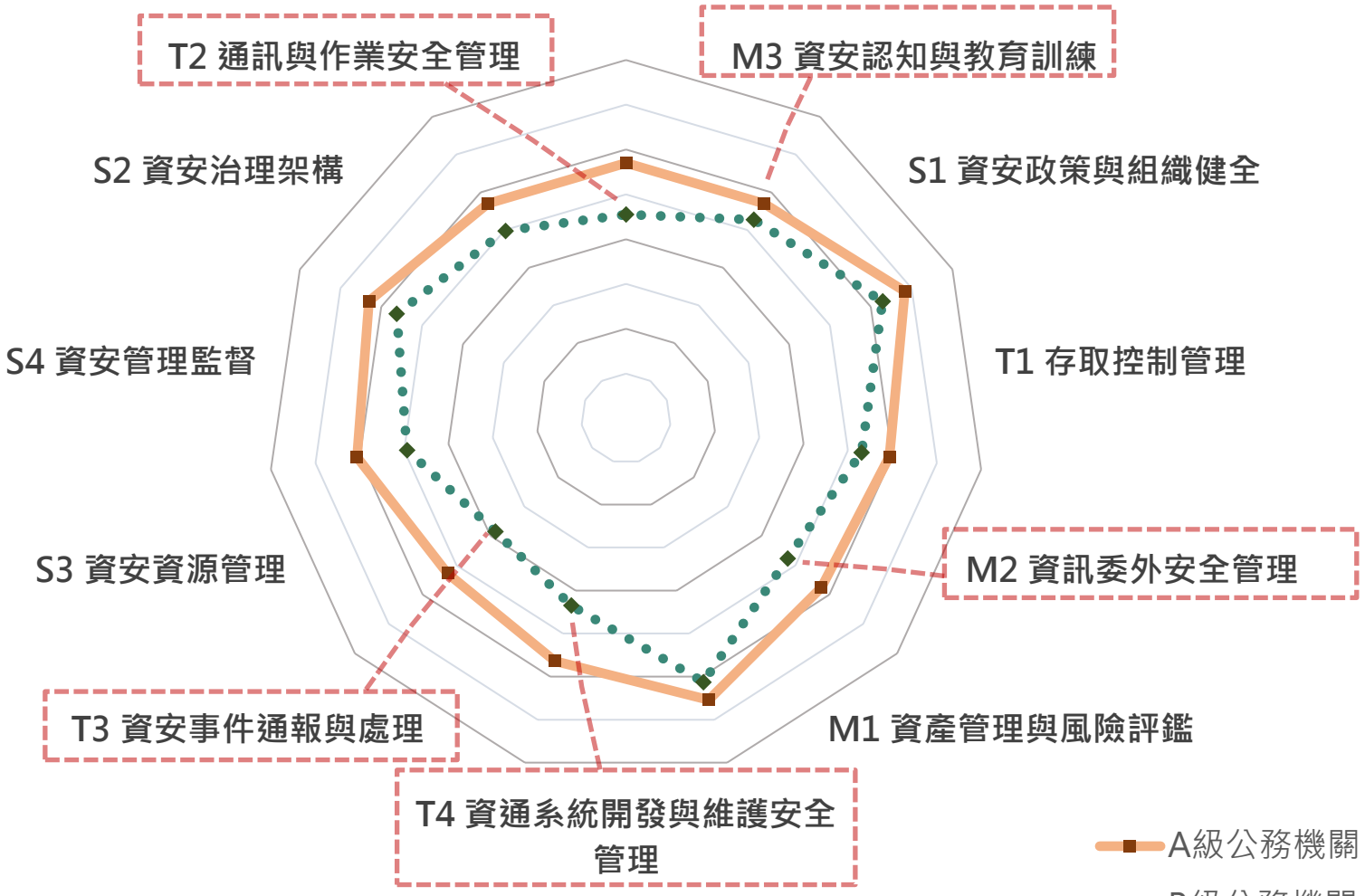
111年度評估概要及相關規範

- 依「**資通安全責任等級分級辦法」應辦事項**規定，資通安全責任等級A級、B級之公務機關，**每年應辦理1次**資安治理成熟度評估
- 依「**國家資通安全發展方案(110~113年)」分年重要進程**
  - **113年**成熟度達成目標：所有**A級政府機關達第3級**以上，80%之**B級政府機關達第3級**以上。



111年度公務機關資安治理成熟度評估結果

各構面平均成績



111年度評估常見項目改善建議

T2	Q33「執行政府組態基準」，建議在機關ISMS文件納入GCB相關程序規範，包含導入程序與例外管理審核機制
T3	Q41「資安事件通報逾時(客觀指標)」，機關應依法定時限完成事件通報、應處及改善作業，並加強人員教育訓練、通報應變演練及檢討
T4	Q45「源碼安全管理」、Q46「區隔系統開發測試及正式環境」等，有待機關落實相關要求並投入資源來加強
M2	Q15「評估委外廠商資安專業能力」，請機關針對委外作業資安管理訂定SOP和文件化要求，建議可參考「政府資訊作業委外資安參考指引」
M3	Q20「機關未能取得符合規定數量專業證照及職能訓練證書」，儘速派員完成受訓及通過評量 (本署112年已增開職能訓練課程)

2.重點工作宣導
2.6績效評核及獎勵作業要點

公務機關資通安全業務績效評核及獎勵作業

- **評核對象分機關及人員**(各評分指標，由本署每年公告之)
  - 機關：分為以下5 組

組別	一	二	三	四	五
資安責任等級	A級	A級	B級	B級	直轄市及各縣市政府
類別	公務機關(無所屬)	公務機關(有所屬)	公務機關(無所屬)	公務機關(有所屬)	

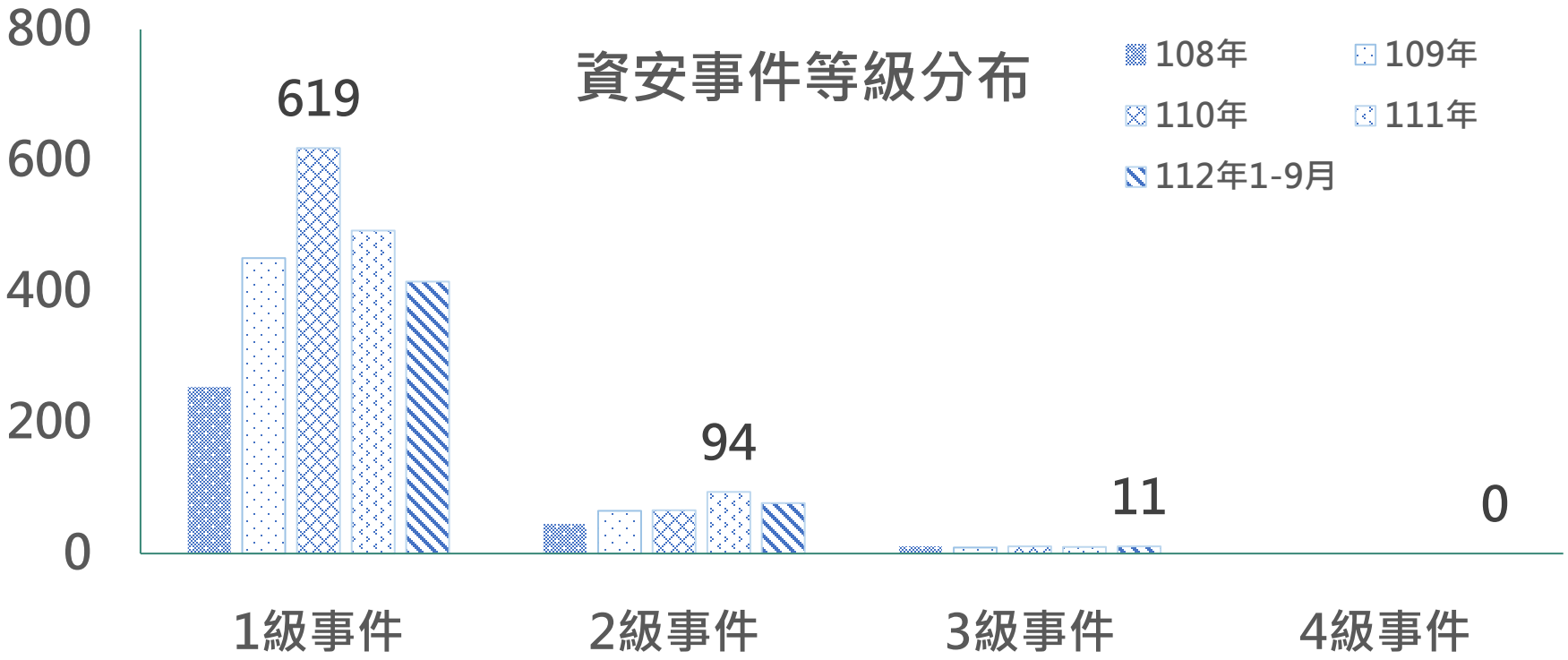
  - 人員：資安責任等級C級以上公務機關資安專職人員。

- **評核項目**：以資安法遵應辦事項、資安管理作業執行情形及其他資安業務促進活動或特殊創新作為原則，包含客觀指標及機關提報資料。
- **獎勵方式**
  - 擇優頒發獎金、團體獎座及個人獎狀
  - 評核分數未達70分者，不列入上開獎勵範圍

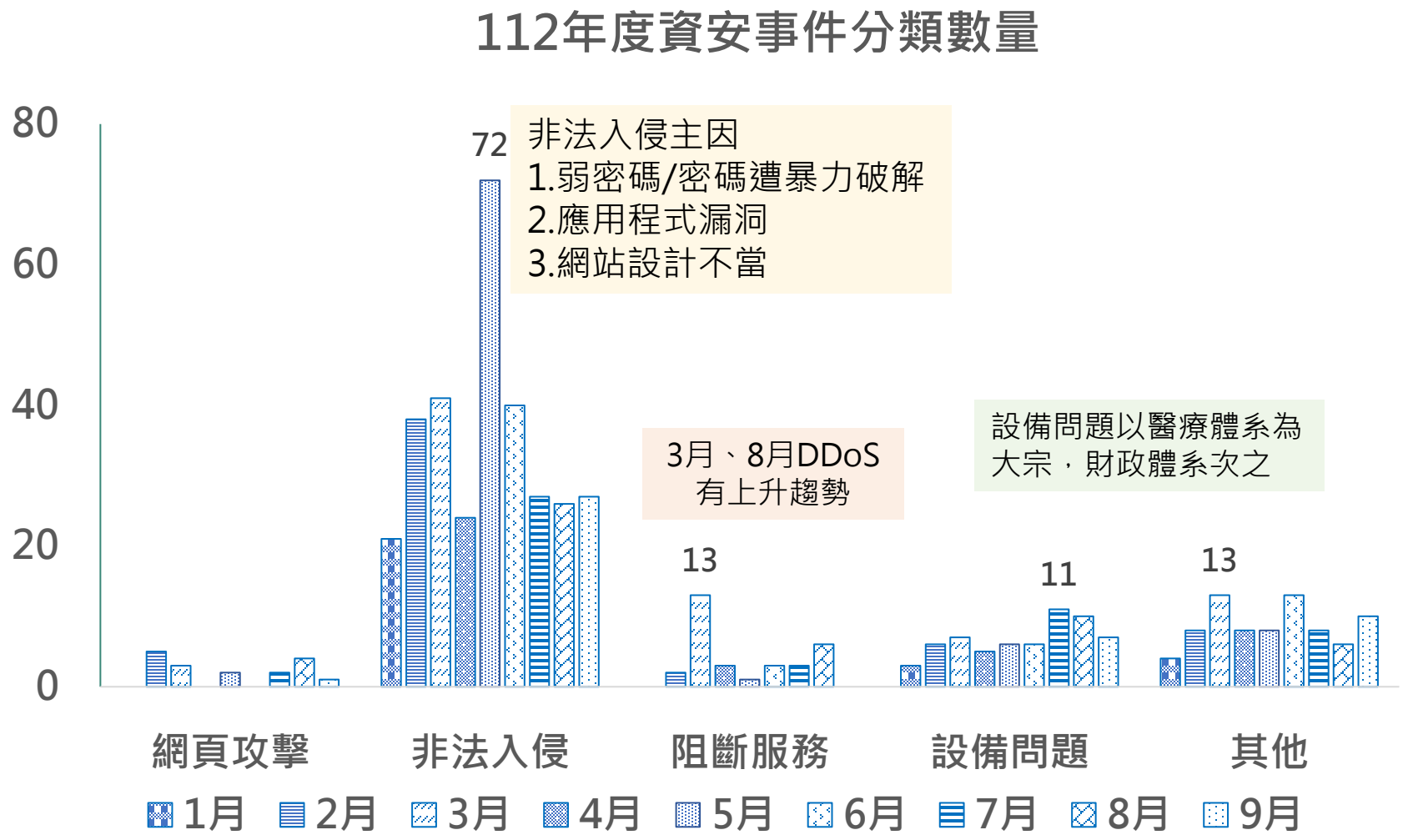
3.近期政府機關資安事件案例分享及防護建議

公務機關資安事件通報統計

- 112年度截至9月底3級資安事件計11件，仍以資料外洩為大宗，另本年度因勒索病毒影響機關核心業務運作情形有增多情形，請注意落實備份資料的有效性及獨立性。

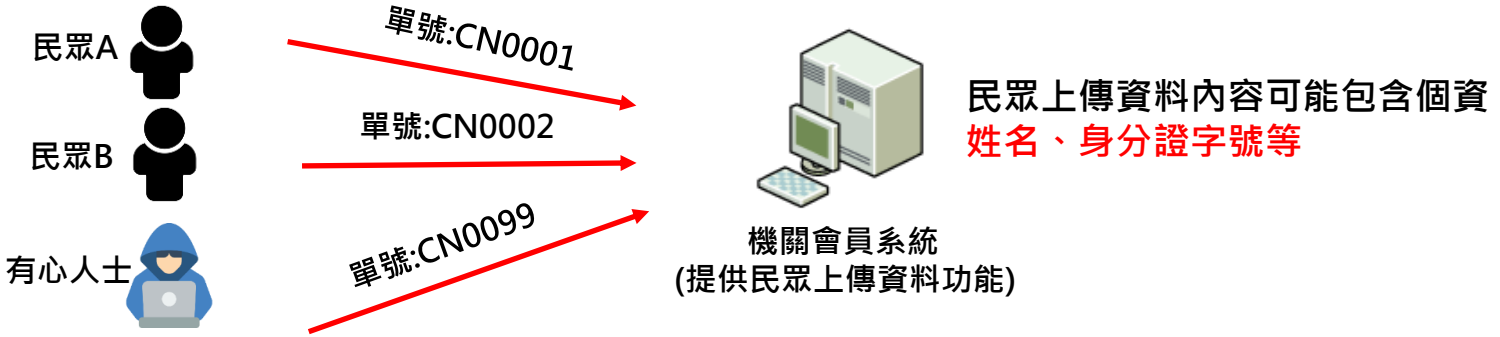


公務機關資安事件通報統計



機關網站驗證機制缺失

- 機關網頁驗證通行碼編號原則相同且易遭猜測(流水號)，又未採多因子認證，有心人士可嘗試登入並取得民眾上傳的資料。



建議防範措施

- 資通系統識別建議啟用**多重認證**機制，如:使用自然人憑證、OTP等
- 依系統防護相關基準採最小權限原則(中、高)，依機關任務及業務功能所需授權存取，**如已無存取需求**應**關閉相關權限(瀏覽、下載)**
- 資料保護：**敏感資料加密儲存**、查詢過程遮蔽及最少揭露

漏洞未修補遭上傳惡意程式

- 機關為民服務系統提供之上傳檔案功能，駭客透過**上傳功能漏洞**植入APT惡意程式，並嘗試取得系統資料，恐有資料外洩之虞

建議防範措施

- 機關應落實軟體及資訊完整性防護，**限制上傳檔案格式**，並對於目錄進行完整性監控及驗證，**即時偵測目錄異動**行為
- 機關辦理重要服務**安全性檢測**作業時，可評估採多家廠商**交互驗證**為宜
- 建立資通安全威脅偵測管理機制(SOC、EDR)

供應商內部資安管理議題

- 機關委託廠商之內部主機，遭攻擊者取得設備控制權，以遠端登錄連線機關系統作業主機進行攻擊，致系統主機伺服器及專用儲存設備遭勒索病毒加密，事件紀錄被清除。

建議防範措施

- 遠端連線原則禁止，例外允許，採VPN(雙因子認證)方式進行遠端維護
- 落實委外廠商管理，必要時進行資安查核
- 如經證實廠商內部受駭，**建議：**

1.甲方提醒乙方通知其他甲方

2.甲方通報本署(依資安事件通報方式)，將評估啟動聯防機制

供應商疏失致網頁驗證功能失效

- 機關系統維運商執行系統更新作業疏失，未發現網頁驗證功能被關閉，學員不需身分驗證即可登入系統，致有心人士可藉此該弱點查看或取得敏感資料，有資料外洩之虞。

建議防範措施

- 落實系統版本更新檢核作業，並應於**測試機完成各角色、各帳號測試後**再上版，應完整確認系統相關檢核驗證功能均正常啟用始可對外開放使用。
- 資料保護：敏感資料加密儲存、查詢過程遮蔽及最少揭露。

近期機關防護重點

落實供應商管理

- ✓ 系統網站更新上版應落實測試作業，並由機關同仁監督。
- ✓ 落實源碼檢測、弱點掃描等作業，並建立弱點修補追蹤機制。
- ✓ 如確認供應商內部受駭，請機關依供應商聯防原則辦理。

強化身分驗證機制

- ✓ 新建帳號第1次以預設密碼登入資通系統時，應有強制變更密碼機制
- ✓ 各帳號之預設密碼不宜相同，另建議提高其預設密碼複雜度
- ✓ 通行碼應避免採用易遭推論方式(如統編、流水號等)進行驗證

勒索病毒防範

- ✓ 網路區段分割，限縮影響範圍
- ✓ 加強內部同仁資安觀念，勿瀏覽不明網頁或點擊惡意連結
- ✓ 並勿下載未經授權軟體
- ✓ 定期執行資料備份(離線備份)，並可快速還原

近期網通設備漏洞說明

- 近期研究人員發現部分機關網通設備存在高風險安全漏洞(CVE-2023-20198)，若啟用網頁介面(Web UI)功能皆會受到影響，包含交換器、無線網路控制器、無線基地台及路由器等本署已於112年10月20日發出ANA漏洞警訊。

國家資通安全研究院
漏洞/資安訊息警訊

發布編號	NICS-ANA-2023-0000453	發布時間	Fri Oct 20 16:44:26 CST 2023
事件類型	漏洞預警	發現時間	Fri Oct 20 00:00:00 CST 2023
警訊名稱	[redacted]存在高風險安全漏洞(CVE-2023-20198)，允許遠端攻擊者在未經身分鑑別之情況下，取得受影響系統之控制權，請儘速參閱官方建議措施		
內容說明	研究人員發現[redacted]之網頁介面存在高風險安全漏洞(CVE-2023-20198)，允許遠端攻擊者在未經身分鑑別之情況下，新增Level 15之高權限帳號，進而利用此帳號控制受影響之系統。該漏洞目前已遭駭客利用，官方正積極修補中，後續更新請參考官網公告。		
影響平台	[redacted]若啟用網頁介面(Web UI)功能皆會受到影響，包含交換器、無線網路控制器、無線基地台及路由器等		
影響等級	高		
	目前Cisco官方尚未釋出更新程式，僅公告建議措施，請參[redacted]官方網頁之「Recommendations」一節，關閉HTTP Server功能或僅允許受信任設備進行HTTP/HTTPS連線，網址如		

- 請各機關盤點存在風險之相關設備，儘速完成更新作業，參考網址https://s.moda.gov.tw/i2TPkMAoVsuL
- 倘無法完成更新，可先進行緩解措施關閉HTTP Server功能，參考網址https://s.moda.gov.tw/r2NNZ4D41MSt

資安事件通報應變演練作業

- 資通安全事件通報及應變辦法18條規定公務機關須配合主管機關規劃辦理資通安全演練作業，其中包括資通安全事件通報及應變演練
- 各機關辦理資通安全事件演練通報，請至國家資通安全通報應變**演練**網站進行相關作業，演練網站如下：
  https://www.ncert.nat.gov.tw/exer/
- **請勿到正式網站進行通報作業，**以維資料正確性

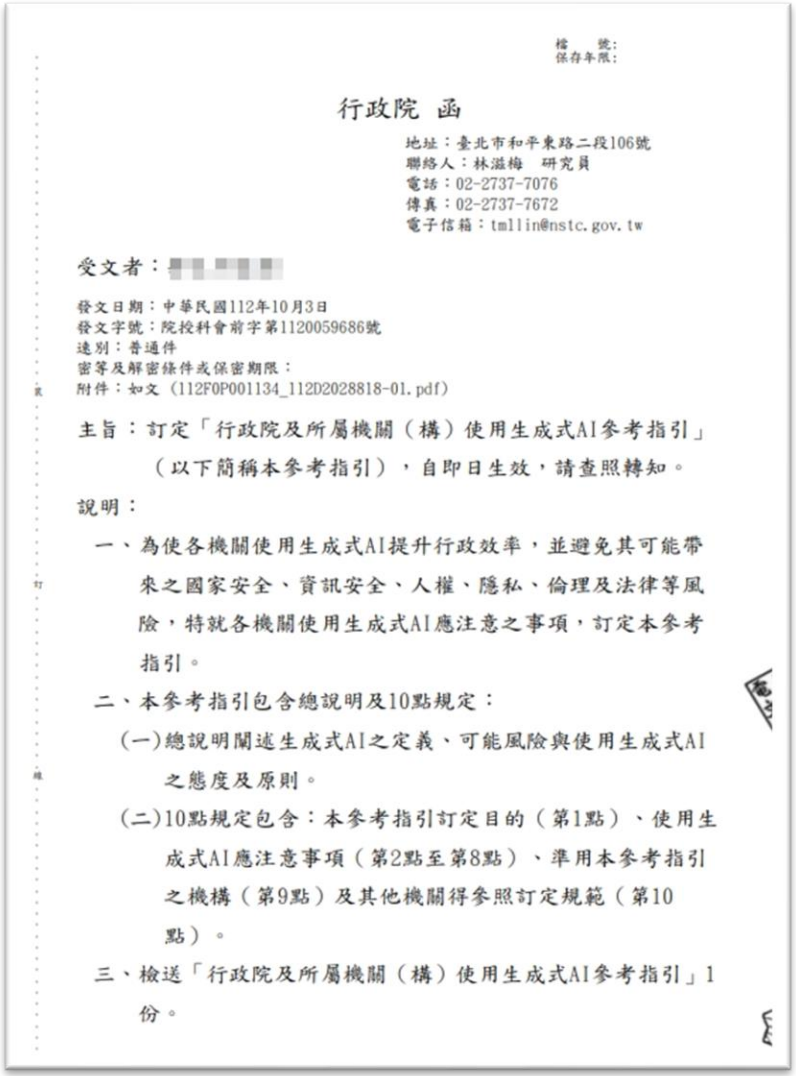
各公務機關使用行動載具注意事項

為強化公務機關使用資通訊產品之軟體安全，**國家資通安全研究院官網\資安規範及報告\共通規範**項下訂有下列指引或注意事項：

- 「**行動裝置資安防護參考指引**」：針對當前行動裝置常見資安風險，提供相關防護措施的建議、安全設定事項，並提供該裝置安全設定檢核表供參。
- 「**行動裝置資通安全注意事項**」：就軟體下載與使用、資料保護、連線功能設定、設定行動裝置密碼自動鎖定功能等，提供使用者防護建議。

各公務機關使用生成式AI注意事項

- 行政院**112年10月3日院授科會前字第1120059686號函**頒**「行政院及所屬機關（構）使用生成式 AI 參考指引」**，簡述如下：
  - 不得向生成式 AI 提供未經機關同意公開之資訊，更不可完全信任生成式 AI 產出之資訊。
  - 各機關得依使用生成式 AI 之設備及業務性質，訂定使用生成式 AI 之規範或內控管理措施。



檔　號:
保存年限:

行政院 函

地址：臺北市和平東路二段106號
聯絡人：林滋梅　研究員
電話：02-2737-7076
傳真：02-2737-7672
電子信箱：tmllin@nstc.gov.tw

受文者：[redacted]

發文日期：中華民國112年10月3日
發文字號：院授科會前字第1120059686號
速別：普通件
密等及解密條件或保密期限：
附件：如文（112F0P001134_112D2028818-01.pdf）

主旨：訂定「行政院及所屬機關（構）使用生成式AI參考指引」（以下簡稱本參考指引），自即日生效，請查照轉知。

說明：

一、為使各機關使用生成式AI提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式AI應注意之事項，訂定本參考指引。

二、本參考指引包含總說明及10點規定：

(一)總說明闡述生成式AI之定義、可能風險與使用生成式AI之態度及原則。

(二)10點規定包含：本參考指引訂定目的（第1點）、使用生成式AI應注意事項（第2點至第8點）、準用本參考指引之機構（第9點）及其他機關得參照訂定規範（第10點）。

三、檢送「行政院及所屬機關（構）使用生成式AI參考指引」1份。

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