資安防護政策及因應措施

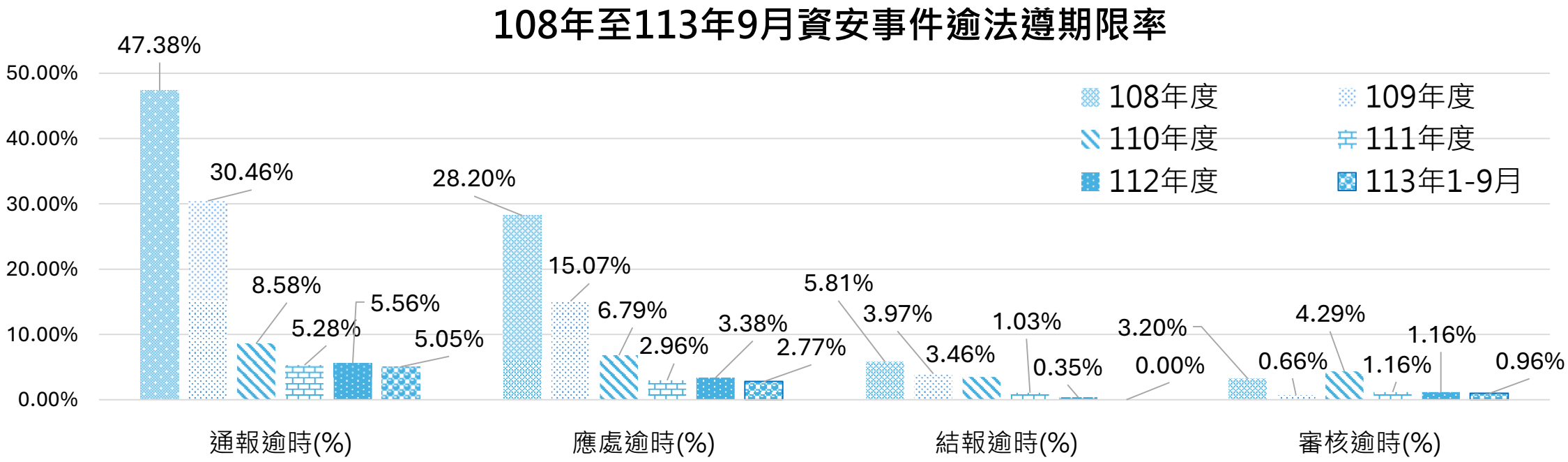
113年11月

報告大綱

1. 政府機關資安事件通報情形
2. 近期資安事件案例分享
3. 近期資安威脅情形
4. SOC精進規劃
5. 黑名單自動化部署服務系統
6. 機關導入零信任(身分鑑別及設備鑑別)參考指引

政府機關資安事件通報情形

政府機關資安事件通報情形



逾時原因與建議措施

1. **加強法遵意識**，如避免應處完成後才進行通報。
2. **落實職務異動交接**，避免因業務人員異動造成通報逾時。
3. **可參考網站操作手冊及落實教育訓練**，使同仁熟悉通報應變網站操作。
4. **落實代理人制度**，避免承辦人不在時資安事件逾時。

近期資安事件案例分享

近期資安事件案例分享 1/7

- 機關FB粉絲專頁遭盜用，經查該專頁管理者為在職員工申請之**私人帳號**，未妥善管理帳號遭盜用(機關已向Meta申訴處理)。

建議防範措施

- 建立**社群平臺帳號管理機制**並**定期審核與帳號清查**，範圍包含機關自建系統、社群平台(FB、IG等)、網站平台(協作平台、blog等)。
- **避免使用弱密碼**，啟用**雙重驗證機制**，並定期更換密碼。
- 定時檢視登入紀錄是否有異常情形。
- 人員異動(離職)**應移除帳號權限**。

帳號盜用佐證建議作法

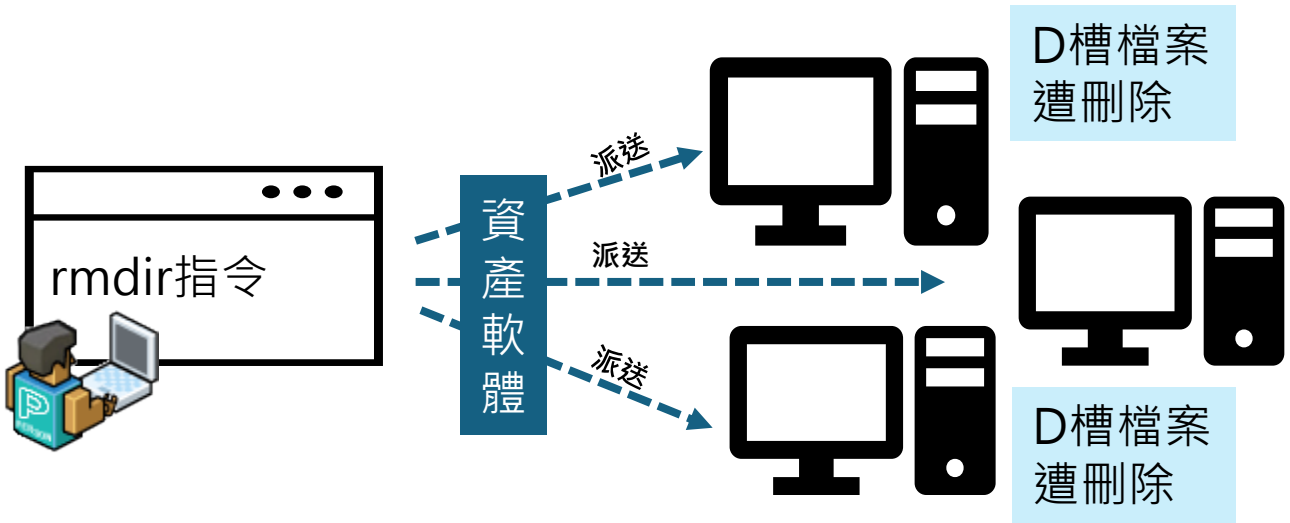
① 至FB官方網頁依指引**取回帳號**(https://s.moda.gov.tw/j9jav2Urbi27)

② **下載登入紀錄方式**(報案佐證)

1) 登入狀態下進入 https://s.moda.gov.tw/CitLheAbVVZA
2) 選擇「帳號安全和登入資訊」，將「你登入的位置」或「登入和登出」中遭盜用時段的登入紀錄畫面擷圖

近期資安事件案例分享 2/7

- 機關委請廠商進行個人電腦維護作業，駐點工程師疑作業疏失**輸入錯誤代碼**，將機關內各科室及所屬單位約300多台的電腦硬碟檔案刪除，執行刪除D槽特定資料夾檔案。



建議防範措施

1. 批次作業前，小範圍測試後再執行，減少錯誤操作造成範圍性影響。
2. 多重審核機制，執行如批次刪除或系統變更等前，宜進行多方審核。
3. 定期備份重要資料。

近期資安事件案例分享 3/7

- 刑事局近期分析詐騙電話來源，係多個學校、機關、企業等使用Tenor AX VoIP Gateway之網路電話交換機(即節費器)遭駭，進而盜用撥打市話，該2007年產品**預設開啟遠端登入(Telnet)，且加密機制不足，駭客透過密碼暴力破解登入。**
- 近期研究人員發現Unix通用列印系統(Common UNIX Printing System，CUPS)異常存取外部印表機服務之連線，存在安全漏洞(CVE-2024-47076、CVE-2024-47175、CVE-2024-47176及CVE-2024-47177)，**未經身分鑑別之遠端攻擊者**可利用漏洞於受影響之Unix作業系統**執行任意程式碼**。

建議防範措施

1. 軟韌體應定期更新及修補漏洞，若已EOS應評估更換設備，避免遭駭侵利用。
2. 落實密碼複雜度、定期變更等密碼安全管控措施。
3. 網通設備關閉不必要開啟之服務及連接埠。

近期資安事件案例分享 4/7

- 今年6月資安業者Sansec警告，知名套件**Polyfill.io**於今年2月易主後，對嵌入該函式庫的網站**植入惡意程式**，並使用相關惡意網域如：cdn[.]polyfill.io等**散播惡意程式**。
- **jQuery 套件**存在**跨站腳本漏洞**(CVE-2020-11022、 CVE-2020-11023)，漏洞分數6.1(CVSS3.1)，可能導致**攻擊者執行惡意程式**

Polyfill相關網域
cdn[.]polyfill[.]io, bootcdn[.]net, bootcss[.]com, staticfile[.]net, staticfile[.]org, unionadjs[.]com, xhsbpza[.]com, union[.]macoms[.]la, newcrbpc[.]com

建議防範措施

1. 建議網站儘速移除Polyfill.io腳本，並避免使用polyfill。
2. 網站避免直接引入CDN線上服務。若有必要，改採其他可靠的CDN 服務
3. 第三方套件定期檢視更新。
4. 評估將惡意網域納入阻擋，檢視設備相關網路是否有惡意網域連線行為，以確認受駭情形

近期資安事件案例分享 5/7

- 某機關委外辦理**推廣活動**，廠商直播過程不慎透漏抽獎網址，有心人透過**該網址即可得知中獎人資訊**，中獎名單含個人資料(包含姓名、手機號碼)，以致敏感資訊外洩。

建議防範措施

1. 直播活動建議預先排演，確認過程中無不當訊息之揭露。
2. 機關辦理**對外活動或公告所使用之系統**時，應**確認其內容之妥適性及其資安管理措施**，避免因系統設計不良致資料外洩。
3. 敏感資訊應**去識別化**，降低外洩風險。

近期資安事件案例分享 6/7

- 機關於官網**公開分享「資安聯防監控月報」**惟月報屬**非公開情資**(TLP:GREEN)，彙集政府資安資訊與內外部情資，僅供機關與資安監控服務廠商作為資安防禦參考，不當公開恐遭他人不當利用。

分享燈號	說明
TLP:RED	資訊的接受者不得與自己以外的其它人分享
TLP:AMBER	資訊內容揭露範圍僅限參與者組織內部
TLP:GREEN	資訊內容可揭露予可明確界定之特定群體
TLP:Clear	資訊內容可公開揭露

Traffic Light Protocol(TLP) 2.0

建議防範措施

1. 機關可參考TLP燈號等級，制定分享標準，定期與同仁宣導，**避免發佈非公開資訊**。
2. 機關公布資訊前，應**制定審核程序，並定期檢視網站資料**，降低非公開資料外洩風險。

近期資安事件案例分享 7/7

- 10月底康芮颱風過境，影響部分地區電力設施，部分機關因電壓供電不穩，致空調設備或主機設備異常，進而影響系統服務。

建議防範措施

1. 機房內設備，無論空調系統、網通設備、主機系統等，皆需配置雙備援及不斷電系統(UPS)或發電機，避免因斷電或供電不穩造成服務中斷。
2. 建置備援機房或雲端備援服務，確保事件發生時可緊急切換，並將電力異常情境納入營運持續演練(BCP)。

近期資安威脅情形

近期資安威脅情形

簡報內容現場展示

SOC精進規劃

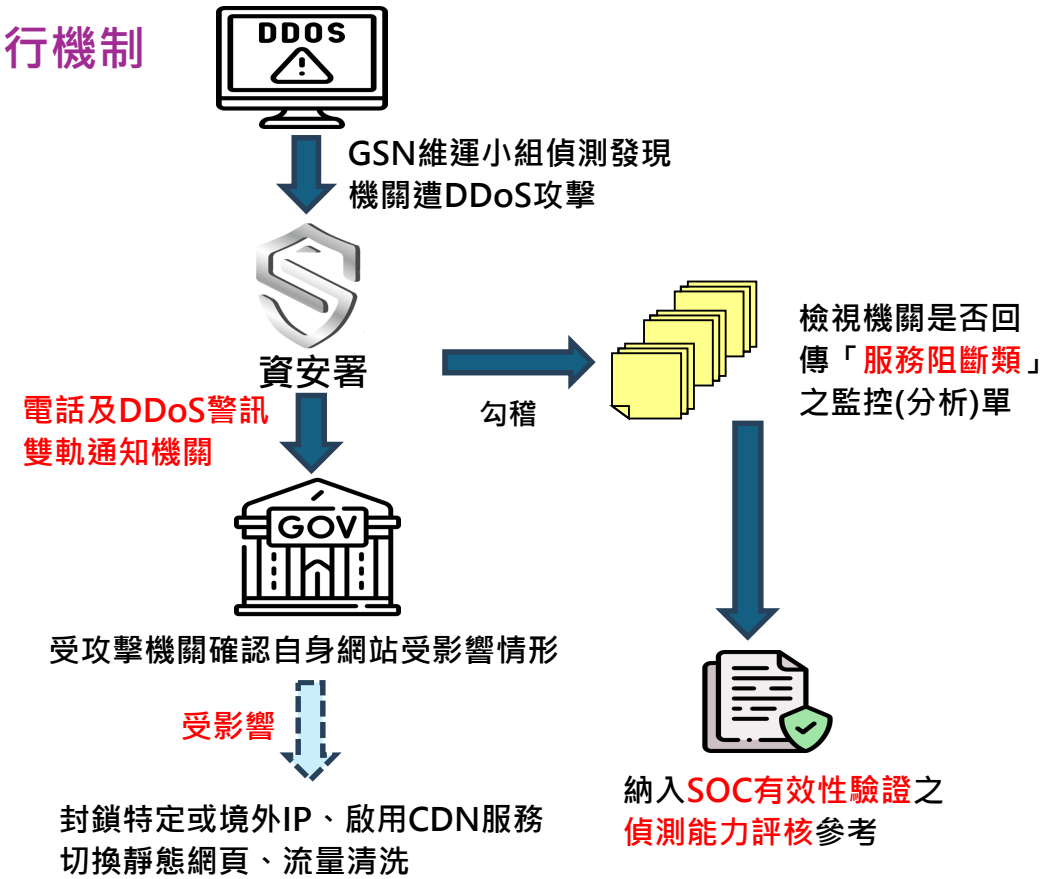
SOC精進規劃1/2

因應近期DDoS攻擊驟增，為強化各機關DDoS偵測應處能力，本署規劃於現行「聯防監控有效性驗證」加入「DDoS攻擊偵測驗證」項目，以提升資安監控能量與品質

擴充聯防監控有效性驗證項目

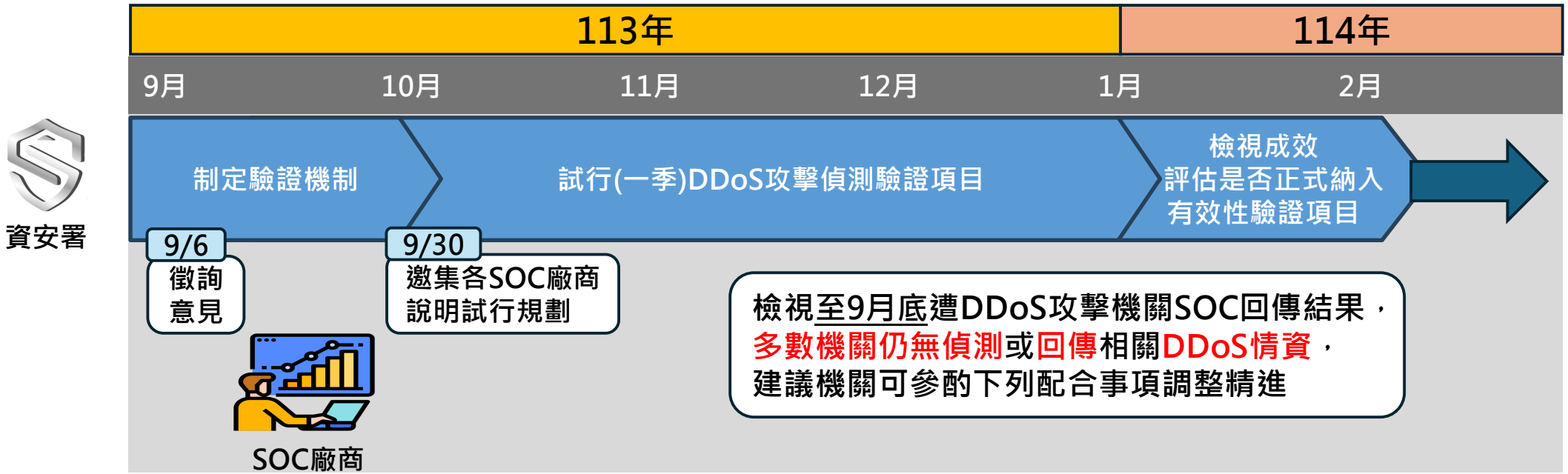
項目	分析指標
1.回傳能力	1.1資安監控情資格式與回傳率
	1.2資安防護項目回傳率
2.偵測能力	2.1網路攻防演練驗證
	2.2資安院資安警訊驗證
	2.3機關通報資安事件驗證
規劃新增	**2.4DDoS攻擊偵測驗證**
3.情資品質	3.1資安監控情資品質分析
	3.2資安監控情資回饋能量

規劃運行機制



SOC精進規劃2/2

- 時程規劃：有關「DDoS攻擊偵測驗證」項目，規劃於本年10月開始試行(3個月)，並於114年1月檢視執行成效，以評估是否正式納入有效性驗證項目



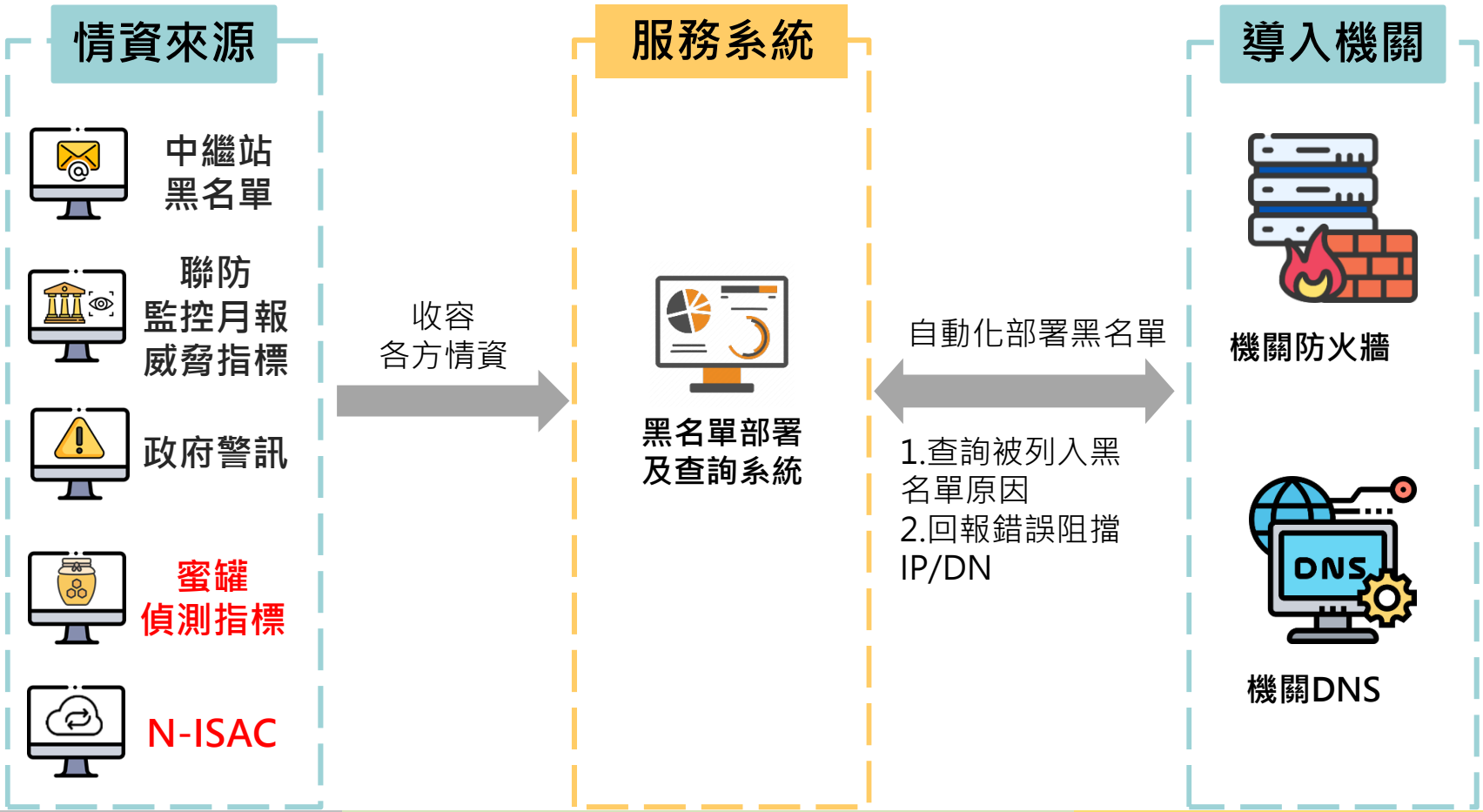
- 機關配合事項：

1. 自建/委外SOC服務，應確認重要服務(如對外網站、DNS服務等)納入資安監控。
2. 依過往基準(baseline)設置具體監控指標，如可用性、回應時間、錯誤碼出現頻率(如404、500錯誤)及流量異常等，及早發現問題並採取相應措施。

黑名單自動化部署服務系統

黑名單自動化部署服務系統1/4

- 為**減輕機關資安人員負擔**與**提升防護即時性**，資安署將已整合之黑名單(**IP清單**與**DN清單**)以**自動化服務**提供予各機關，可應用部署於防火牆與DNS



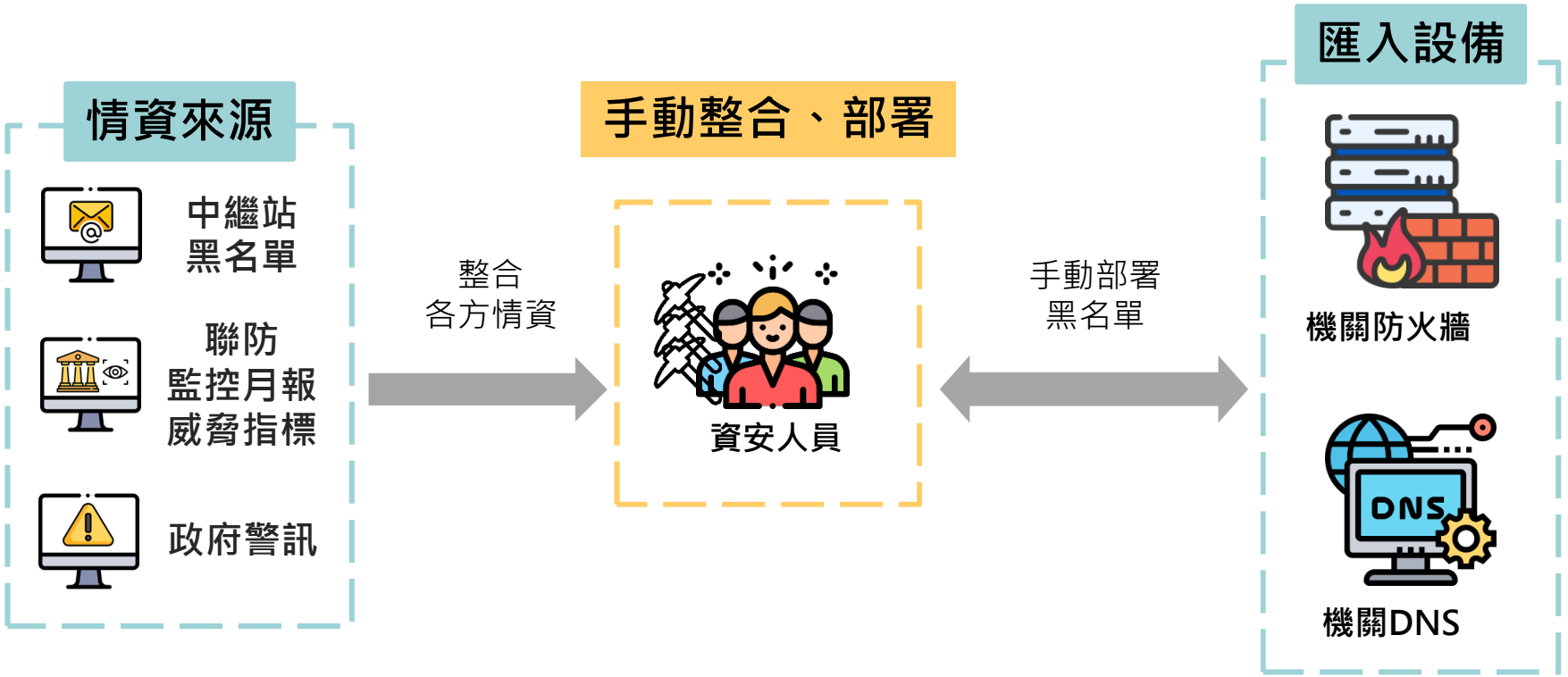
黑名單自動部署服務系統-情資來源說明2/4

- 不同於資安廠商與開放情資，資安署所整合之黑名單包含特別針對**政府機關**進行可疑行為或惡意威脅指標，**每日更新黑名單資料**

情資名稱	情蒐來源	提供內容
中繼站黑名單	• 政府骨幹網路惡意電郵機制 • 政府機關惡意電郵偵測機制	資安院中繼站黑名單 – IP位址(IoC) – DN域名(IoC)
蜜罐偵測指標	• 外網蜜罐部署點之誘捕資料、國內外蜜罐情資	蜜罐偵測之網路攻擊威脅 – IP位址(IoA)
聯防監控月報威脅指標	• A、B級公務機關監防監控工單 • 政府骨幹網路偵測	資安聯防監控月報 – IP位址(IoC) 、(IoA) – DN域名(IoC)
政府警訊	• 資安院發送至政府機關之INT警訊，警訊單內之惡意IP	警訊中之受駭偵測指標 – IP位址(IoC) – DN域名(IoC)
N-ISAC	• 統整國內外資安情資與國際資安組織通報以產製威脅清單	情資中之受駭偵測指標 – IP位址 (IoC/IoA) – DN域名(IoC/IoA)

未申請黑名單自動部署服務系統-手動更新3/4

- 未申請服務機關需**手動整合**多方資訊且**無自動更新**，情資來源主要來自
  - 中繼站黑名單：公布於通報應變網站
  - 聯防監控月報威脅指標：公布於通報應變網站
  - 政府警訊：僅產生可疑連線之機關可得知該資訊



黑名單自動部署服務系統-申請及部署方式4/4

- 113年推辦黑名單自動化部署服務系統，7月17日邀請**資通安全責任等級A級、B級公務機關**參加線上說明會，8月1日開放申請服務，經統計30個A級機關、53個B級機關完成部署，如欲申請者請於**11月30日前至資安人員身分驗證系統(iAuth)**申請，後續將開放**資通安全責任等級C級公務機關申請**。

- 機關配合事項：首次登入黑名單自動部署服務，需設定**防火牆基本資訊**，如防火牆廠商、型號及防火牆外部IP；以及防火牆列表中**IP/DN黑名單清單使用之Token**作為防火牆存取黑名單之路徑，將其複製至各防火牆阻擋設定，上述步驟**僅需設定1次**即可，後續以排程方式每日自動更新黑名單資料。

機關導入零信任(身分鑑別及設備鑑別)參考指引

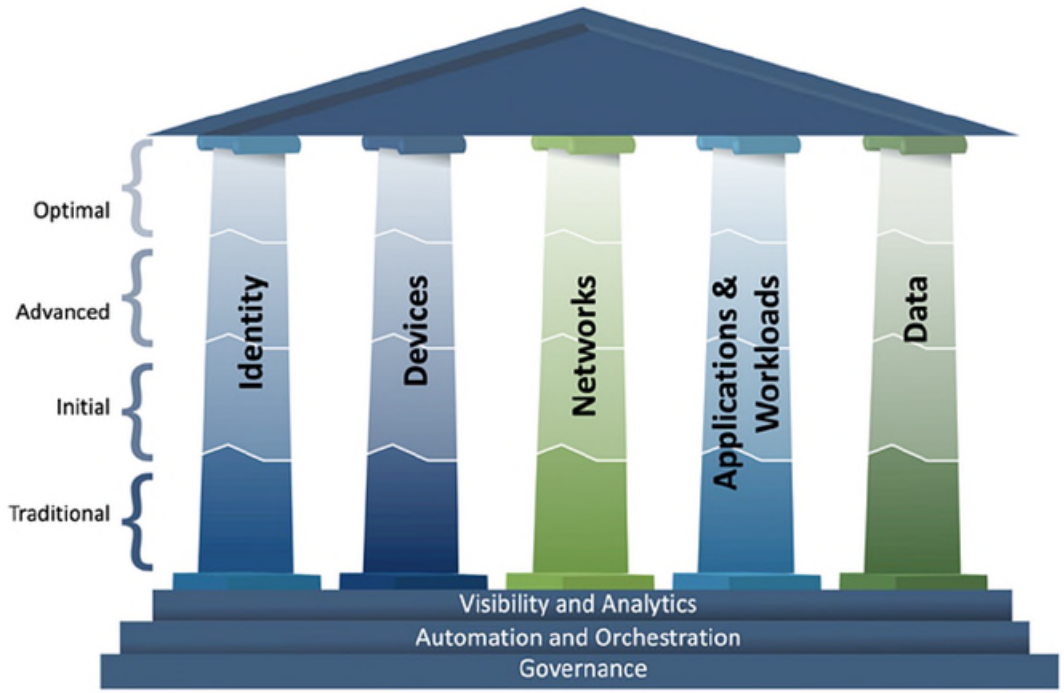
零信任架構簡介1/6

我國政府零信任架構包含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

CISA零信任成熟度模型2/6

美國網際安全暨基礎設施安全局(CISA)於2023年4月發布零信任成熟度模型(Zero Trust Maturity Model, ZTMM) 2.0版本，說明包含五大支柱各階段之安全要求



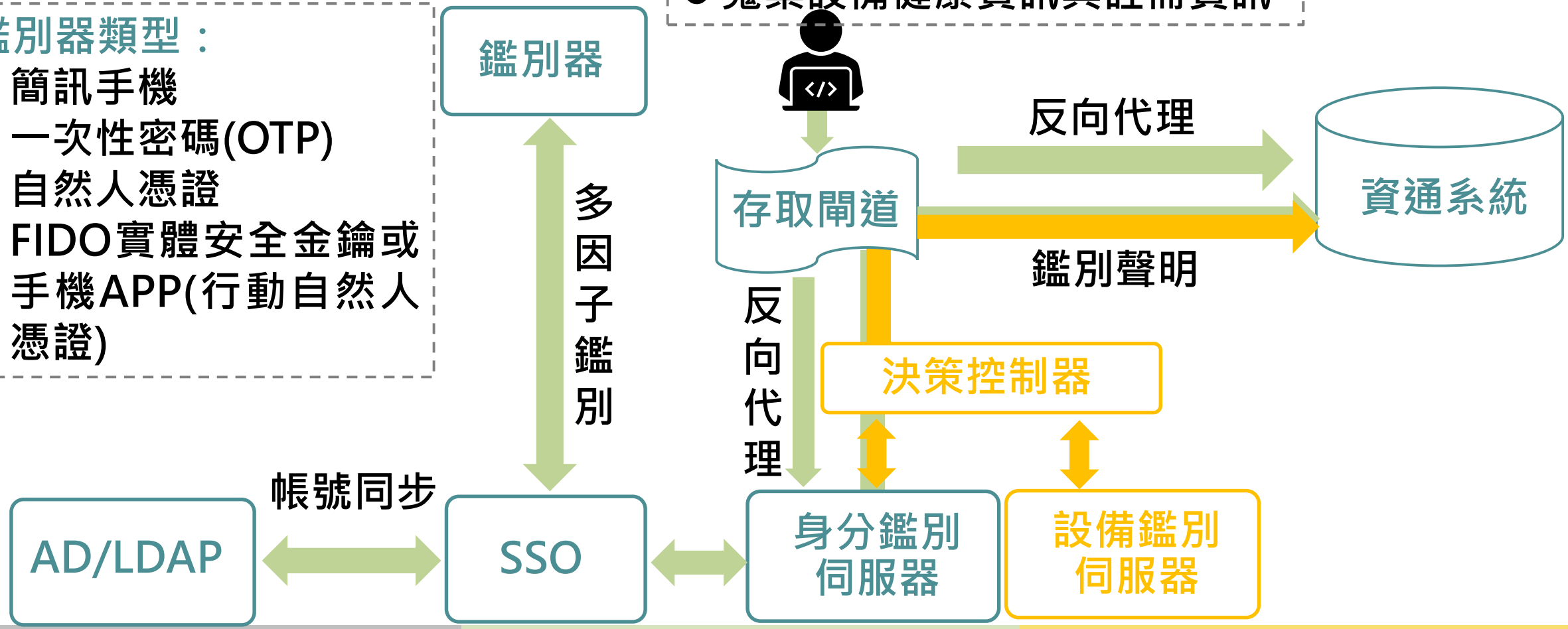
- **傳統階段**：零信任相關配置與政策執行主要依賴手動操作，尚未引入政策執行的自動化機制，安全政策是靜態的，支柱彼此之間的政策設定獨立
- **初始階段**：開始政策執行的自動化並可跨支柱支援，以及具有基本的可視性
- **進階階段**：具備自動化控制機制，統一身分鑑別與存取控制，集中化的可視性，並可根據風險動態調整權限
- **最佳化階段**：政策可自動調整，動態最小權限存取管理，實現即時的資產與資源的屬性分配，並且具有全面威脅態勢感知與集中可視性

本指引以零信任成熟度初始階段為參考基礎歸納出身分鑑別與設備鑑別之必要功能

政府零信任架構- 身分與設備鑑別3/6

使用端設備：
- 安裝代理程式
- 蒐集設備健康資訊與註冊資訊

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(行動自然人憑證)



零信任身分與設備鑑別必要功能4/6

- 零信任導入指引參考CISA零信任成熟度之初始階段要求，歸納出身分鑑別與設備鑑別必要功能

身分鑑別

1. 部署身分鑑別伺服器
2. 整合現有帳號身分鑑別
3. 存取授權有效期
4. 身分鑑別伺服器管理介面
5. 身分鑑別最小授權原則
6. 日誌保存與查詢介面
7. 存取閘道管控
8. 反向代理

設備鑑別

9. 部署設備鑑別伺服器
10. 設備鑑別機制
11. 設備鑑別伺服器管理介面
12. 設備鑑別伺服器整合介面
13. 身分與設備鑑別最小授權原則

共通性項目

14. 通訊加密
15. 資安檢測

導入程序：規劃、執行、檢查5/6

規劃

- 機關環境與需求盤點
- 流程設計

執行

- 防火牆、DNS組態設定
- 身分鑑別組件部署與資通系統介接
- 設備鑑別組件部署與決策控制器整合
- 日誌保存

檢查

- 自檢15項查檢項目

指引功能實作及驗證說明範例6/6

以身分鑑別第1項功能為例：部署身分鑑別伺服器

FAQ：
系統無法正常解析鑑別聲明，或者只支援一種身分驗證機制

功能說明			
雙因子鑑別	• 通過身分鑑別後，產生具簽章與加密的鑑別聲明	• 身分鑑別伺服器對資通系統發出具簽章與加密的鑑別聲明，資通系統須可解密與解析鑑別聲明	• 截圖佐證雙因子或無密碼驗證之身分鑑別 • 資通系統顯示解密後之鑑別聲明屬性，如Session expire time之佐證截圖

檢查身分鑑別伺服器的配置，確保其支援並啟用多因子鑑別

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