許權廣

數發部資安職能講師

醫協智慧醫療委員

陽明交大竹銘醫院資訊長

教育部資安稽核委員

臨床護理師

多維度的資安管理需求


CYBERSEC
DATA CENTER
✓ 資通安全法
SO 27001
✓ 認證
✓ NIST
框架
落實
資安政策每年評估
資產管理定期清查
資安組織定期稽核
資安事故擬真演練
資訊核心定期演練
資安教育與時俱進


資通安全法
相關要求
搞定
ISO 27001
相關要求
NIST
框架指引
要求

NIST 2024資安框架2.0的創新與擴展

治理 (Govern)

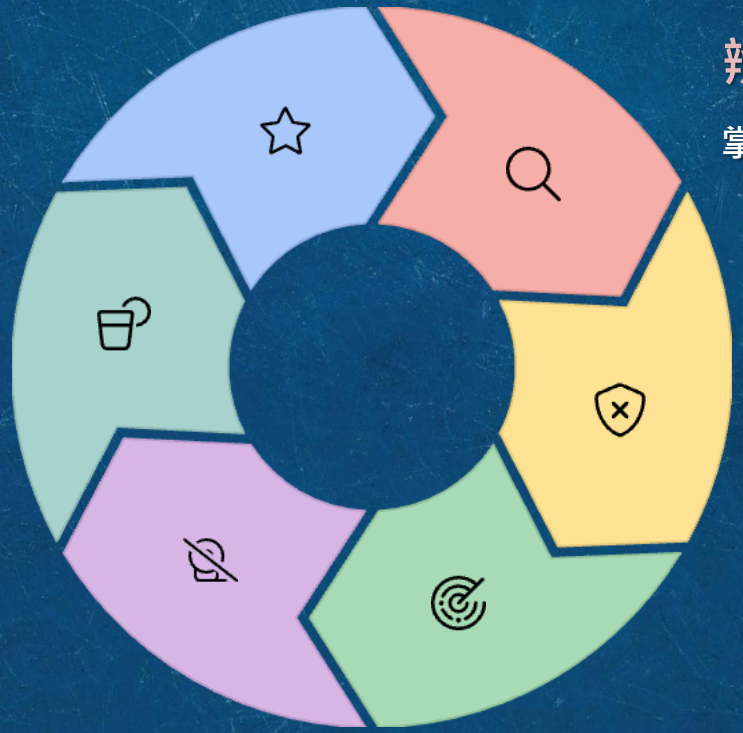
制定組織資安策略與執行方針，強調高層領導在資安管理中的關鍵角色

復原 (Recover)

系統復原與持續改進，確保營運持續性

應變 (Respond)

事件處理與調查，有效應對安全事件並降低影響



辨識 (Identify)

掌握資產與風險評估，識別關鍵系統與潛在威脅

保護 (Protect)

實施防禦機制，建立全面性的安全控制措施

偵測 (Detect)

監控與異常檢測，即時發現潛在的安全事件

原本主要針對關鍵基礎設施，擴大至各種規模和類型的組織

醫院資安的完整防禦架構

核心到週邊

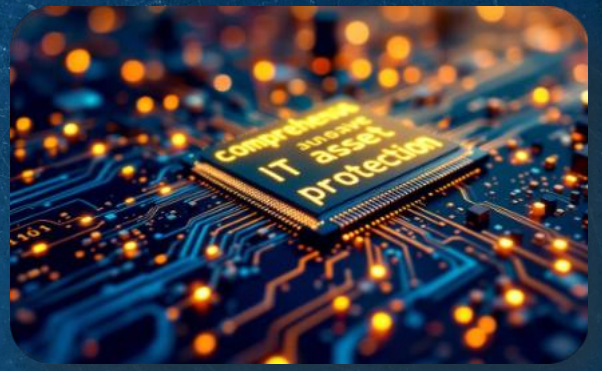
保護關鍵系統和資料，防止外部威脅入侵

- 資料庫防護 DB Protect
- 安全事件監控與分析 SIEM
- 內外防火牆 Firewall
- 入侵偵測與防禦 IDS/IPS
- 網域/進階防護 DNS Protect/APT
- 應用程式防火牆 WAF

個人到群體

確保使用者和設備安全，防止內部風險

- 多因子驗證 MFA
- 帳號與身份管理 IAM
- 資料外洩防護 DLP
- 網路存取控制 NAC
- 雲端安全閘道 Cloud Proxy, CASB
- 特權帳號管理 PAM



軟體到硬體

從軟體應用到硬體設備，全面保護資產

- 郵件.社交工程.防毒 MSA
- 端點偵測與回應 EDR/XDR
- 行動裝置管理 MDM
- USB 控管、BIOS 保護 Firmware
- 物聯網醫療設備 IoMT Protect
- 零信任存取 ZTNA

多層防禦的整合與協同思考

第一道防線：郵件安全閘道攔截釣魚郵件

在郵件進入內網前過濾惡意內容

第二道防線：端點EDR阻止惡意程式執行

即使惡意內容到達端點，EDR仍可偵測並阻止執行

第三道防線：內網區隔限制橫向移動

即使端點淪陷，內網區隔防火牆也能限制其橫向移動

第四道防線：SIEM/SOC持續監控與響應

安全團隊透過集中監控平台發現並處理突破前三道防線的威脅

CISO應該要思考的問題

買了EDR，是否有足夠人力反應?
預算有限，部署的點位是否正確?
還沒裝的，是否可以做什麼補強?

至少確保沒裝的無法到SERVER段

防火牆幾百條規則，是否有疏漏?
如果只買了外部防火牆，怎麼辦?
怎麼確保只動其一，不影響其二?

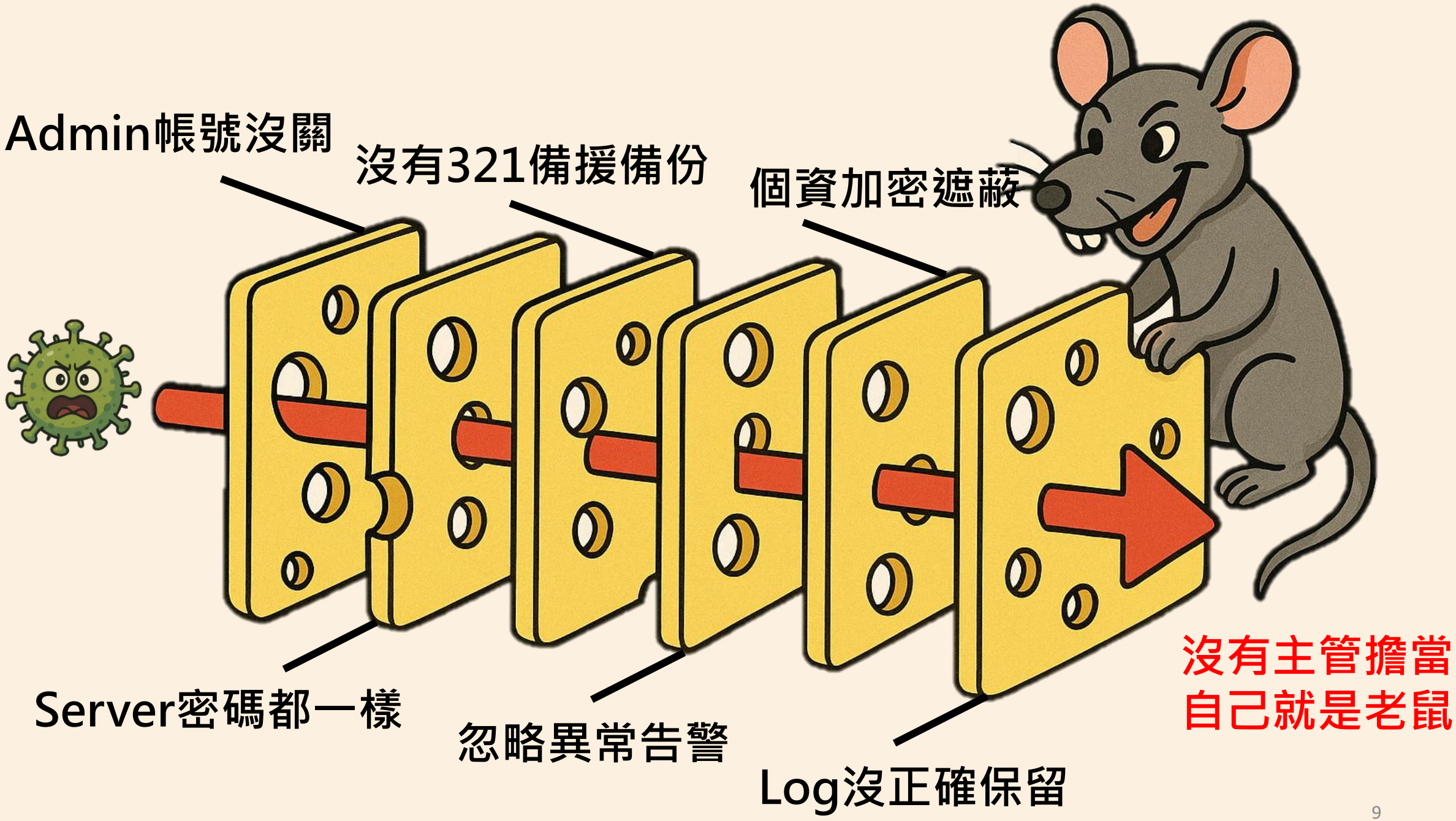
至少確保關閉境外連線

雙因子驗證預算不足，分配給誰
廠商都只用同一帳號，連入維護
沒有側錄軟體稽核維護存取內容

至少人工驗證.螢幕錄影.關Admin

資安教育訓練無法有效確認成果
廠商安排的技術訓練同仁聽不懂
錯誤的部署導致團隊面臨高風險

至少要有履約保證或第三方支援


Admin帳號沒關
沒有321備援備份
個資加密遮蔽
Server密碼都一樣
忽略異常告警
Log沒正確保留
沒有主管擔當
自己就是老鼠

從傳統看正確的資安治理方向

傳統安全模型的缺陷

邊界防護模型

機構使用防火牆等設備保護外部邊界，
內部防護相對薄弱。

木馬屠城風險

攻擊者一旦突破邊界，可能直接進入內部系統，造成重大損害。

邊界模糊化

自攜設備、雲端服務
使傳統邊界界定變得困難。

遠距工作挑戰

遠距醫療趨勢使得
系統不再侷限於醫院內部。

零信任架構的緣起

1

2003年

Jericho Forum開始探討「去邊界化」趨勢，質疑傳統邊界防護模式。

2

2010年

Forrester首席分析師John Kindervag正式提出「零信任」概念。

3

2020年

美國NIST頒布標準文件「SP 800-207：零信任架構」。

4

2020年後

疫情推動遠距工作與醫療，加速零信任發展與應用

零信任的基礎概念

核心理念

永不信任，始終驗證

身分驗證

持續確認使用者身分

設備驗證

確認設備合規性和健康與更新狀態

最小權限

僅提供完成任務所需的最低權限

持續監控

全程追蹤所有存取行為

零信任架構的核心要素

進階身分治理

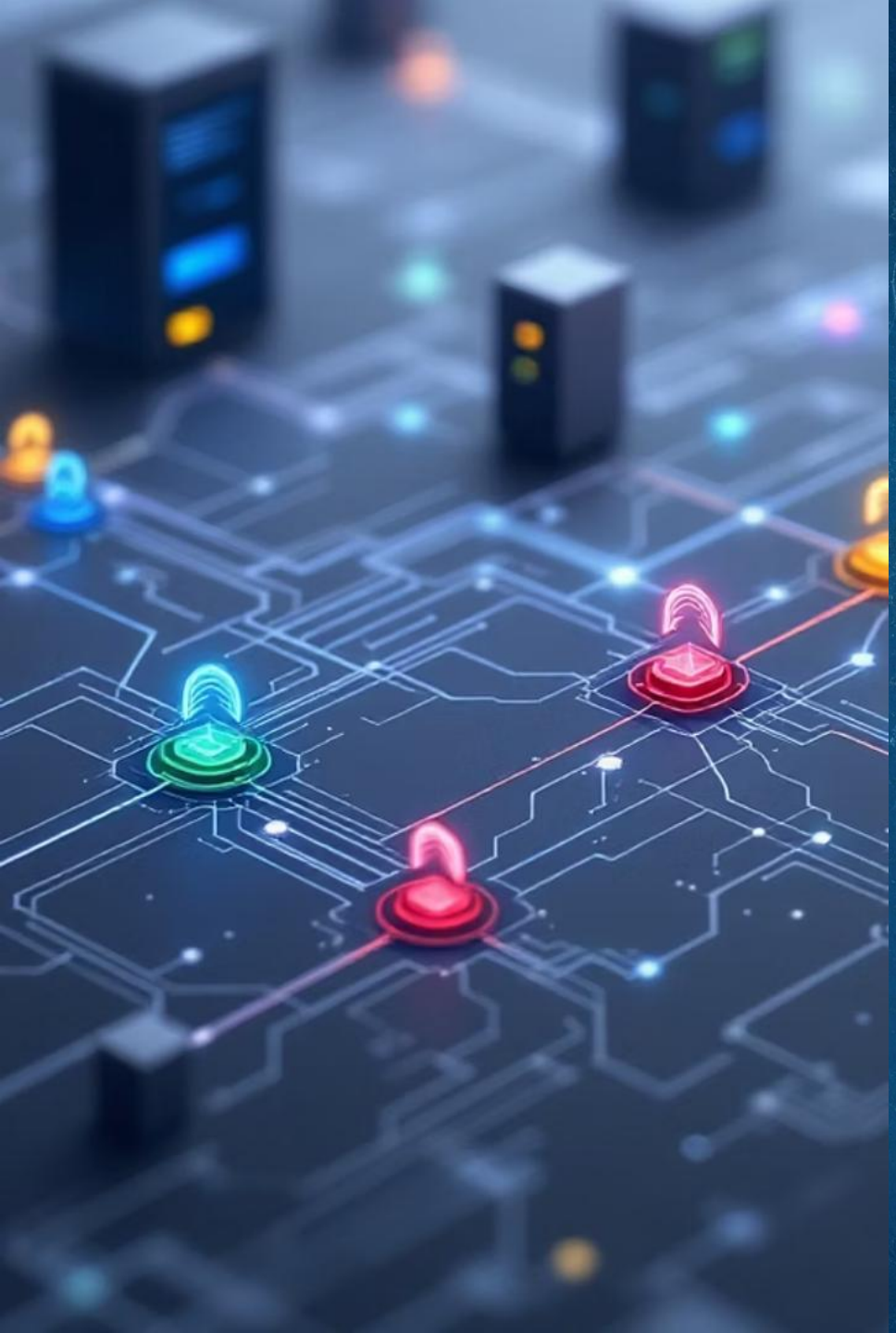
強化身分驗證，確保身分真實性和可靠性

網路微分割

將網路劃分為細小安全區域，限制橫向

軟體定義邊界

動態創建安全連接，隱藏資源減少攻擊面



我國零信任架構推動現況

國家政策支持

「國家資通安全發展方案」已將零信任列為重點工作項目。

政府機關導入

採用資源門戶部署模式，確保資通系統的安全存取。

金融機構應用

金管會「金融資安行動方案2.0」將零信任納入推動重點。

廠商產品驗證

至2023年已有多項身分與設備鑑別產品通過驗證。

零信任三大核心機制

身分鑑別

雙因子硬體加密鑑別，強化身分驗證

設備鑑別

僅有已註冊且更新的設備可連線存取

信任推斷

據信任分數，決定最終資源存取權限

醫療可以先從特殊病房或高單價醫療開始建立相關環境

法規的遵循 與 策略的訂定

法規名稱：資通安全責任等級分級辦法 EN

修正日期：民國 110 年 08 月 23 日

法規類別：行政 ＞ 數位發展部 ＞ 資通安全目

附檔：

- 附表一 資通安全責任等級A級之公務機關應辦事項.PDF
- 附表二 資通安全責任等級A級之特定非公務機關應辦事項.PDF
- 附表三 資通安全責任等級B級之公務機關應辦事項.PDF
- 附表四 資通安全責任等級B級之特定非公務機關應辦事項.PDF
- 附表五 資通安全責任等級C級之公務機關應辦事項.PDF
- 附表六 資通安全責任等級C級之特定非公務機關應辦事項.PDF
- 附表七 資通安全責任等級D級之各機關應辦事項.PDF
- 附表八 資通安全責任等級E級之各機關應辦事項.PDF
- 附表九 資通系統防護需求分級原則.PDF
- 附表十 資通系統防護基準.PDF

※歷史法規係提供九十年四月以後法規修正之歷次完整舊條文。

※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革

附表十 資通系統防護基準七構面

構面一
存取控制 3 項

		控制措施內容 (主管需引導訂定規範)
帳號管理	高	一、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。 二、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。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號異常使用時回報管理者。 五、等級「中」之所有控制措施。
	中	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。
	普	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。

最小權限	控制措施內容 (主管需引導訂定規範)
高 中	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。
普	無要求。

遠端存取	控制措施內容 (零信任之前，需訂定規範)
高 中	一、遠端存取之來源應為機關已預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。
普	一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 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。

構面二
事件日誌與可歸責性 5 項

資通系統日誌管理系統設計(儲存.異動)

系統目標

- 確保系統操作的可追溯性，支援事件歸責、稽核取證及法規合規性要求。
- 確保日誌的完整性、機密性和可用性，支援日誌的收集、存儲、檢索、清除和備份。
- 提供異常行為監控及警示功能，及時發現並回應潛在威脅。

系統範圍

- 作業系統日誌（OS Event Log）：記錄系統啟動、登出、系統錯誤和系統資源使用等關鍵事件。
- 網站日誌（Web Log）：記錄HTTP請求、用戶訪問行為、錯誤狀態和訪問來源等。
- 應用程式日誌（Application Log, AP Log）：記錄業務交易、使用者操作和應用程式異常等信息。
- 登入日誌（Logon Log）：記錄使用者登入、登出、登入失敗等與身份驗證相關的事件。
- 開源工具：Elasticsearch + Kibana

日誌記錄內容與儲存容量	控制措施內容 (主管訂定檢查機制)
高	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。
中	
普	依據日誌儲存需求，配置所需之儲存容量。

LOG類型要盡可能完整，以確保資安事件發生時有明確歸責

日誌處理失效之回應

控制措施內容

高	一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。
中	
普	資通系統於日誌處理失效時，應採取適當之行動。

日誌的形成跟保存跟不可改，均是處理失效的判斷依據，應設計監控機制或定期查核

時戳及校時	控制措施內容
高	一、系統內部時鐘應定期與基準時間源進行同步。 二、等級「普」之所有控制措施。
中	依據日誌儲存需求，配置所需之儲存容量。
普	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。

雲端系統不容易產生此錯誤，但是不同系統間容易疏忽，應有內部查檢表確認

日誌資訊之保護	控制措施內容
高	一、定期備份日誌至原系統外之其他實體系統。 二、等級「中」之所有控制措施。
中	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。
普	對日誌之存取管理，僅限於有權限之使用者。

日誌最怕被勒索病毒破壞，除了遵循備份機制，也要確保運用雜湊值比對檔案一致性

構面三
營運持續計畫 2 項

	控制措施內容	
系統備份	高	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。
	中	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。
	普	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。

遵循三二一備份原則，即使受攻擊也能快速還原，也應主動與診所約定演練時間

		控制措施內容
系統備援	高 中	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。
	普	無要求。

相關計畫應包含硬體設備若故障，診所是否熟悉替代方案之運作

構面四
識別與鑑別5項

內部使用者之識別與鑑別

	控制措施內容
高	一、對資通系統之存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。
中	
普	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。

		控制措施內容
身分驗證管理	高 中	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。
	普	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。(或FIDO) 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。

鑑別資訊回饋&加密模組鑑別	控制措施內容
高	
中	資通系統**應遮蔽鑑別過程中之資訊**。 資通系統如以密碼進行鑑別時，該**密碼應加密或經雜湊處理**後儲存。(鑑別之中高)
普	非內部使用者之識別與鑑別：資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。

構面五
系統與服務獲得 8 項

安全軟體設計參考指引 (安全設計原則)

- **縱深防禦**

  例如：身份認證機制、輸入驗證機制、簡單錯誤訊息，這樣採用多重安控設計，單一措施被突破或失效只造成部分危害。

- **最小權限**

  各角色或可能存取物件的程序或外部元件，必須對功能與資料的權限都設定為必須的、最小的權限。

- **最少共用**

  盡可能減少適用於所有使用者或角色的機制，譬如前台後台登入身分驗證分開，避免攻擊者嘗試登入後台。

安全軟體設計參考指引 (安全設計原則)

- **權限分離**

  避免單一人員或主體的行為對整個系統帶來重大傷害。

- **完全仲裁**

  外界任何請求，必須完完整整地檢查過每一個請求，才能讓它流進來，存取系統內的資源。特別針對重要物件或功能之存取，重新要求身分認證及授權，以避免重送攻擊的危害。

- **可接受度**

  安全機制常會影響到易用度，使得步驟增加或是額外的動作，但應該儘量將影響最小化在合理範圍內。

安全軟體設計參考指引 (安全設計原則)

- **安全故障**

  發生錯誤時，各項安全機制(如存取控制、加密資訊、輸入驗證、日誌紀錄)應該處於有效的狀態。

- **簡化設計**

  例如：模組化設計、可重複使用的元件、減少不必要的功能，這樣Keep It Simple Stupid，比較不容易產生安全漏洞。

- **使用現存元件**

  重複使用現有的、經過安全測試或實證的元件，以避免增加新元件所產生的風險。

安全軟體設計參考指引 (安全設計原則)

- **防範單點失效**
  採用叢集或負載平衡等方式，當系統中單一點發生失效時，其他點可以接手或持續作業。
- **開放設計**
  不應是基於假設別人不知道程式碼安全作法為何。
- **最弱環節**
  攻擊者較可能攻擊軟體中的脆弱點，整個系統的安全性等同於最弱元件的安全性。

安全軟體設計參考指引 (執行攻擊面分析)

- **定義攻擊面**

  攻擊者可能進入系統並取得所需資訊的各種不同進入點，例如資料/命令進出所有路徑、保護系統資源路徑或資料的功能、程式執行中洩漏的金鑰/機敏資料/個資、匿名使用者存取權限、權限過高的管理帳號。

- **攻擊面識別**

  從攻擊者的角度審查設計文件，透過原始碼識別攻擊者各種進入/離開的點，例如登入/驗證、管理界面、查詢和搜尋功能、業務流程、 API介面等。

安全軟體設計參考指引 (執行攻擊面分析)

- **攻擊面評估**

  識別出高風險區域，並專注在遠端進入的攻擊點，了解可以導入何種合適之控制措施來保護系統。

- **攻擊面風險管理**

  通常隨著加入更多介面、使用者類型、和其他系統整合，會增加應用程式的攻擊面。可以透過簡化模型(例如：降低使用者層級的數量或是不儲存不必要儲存的資訊)，將未使用之功能關閉或導入操作控制(例如應用程式防火牆等)來降低攻擊面。

系統發展生命週期開發階段	控制措施內容
高	一、執行「源碼掃描」安全檢測。 二、系統應具備發生嚴重錯誤時之通知機制。 三、等級「中」及「普」之所有控制措施。
中	
普	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。

系統發展生命週期測試階段	控制措施內容
高	一、執行「滲透測試」 二、等級「中」及「普」之所有控制措施。
中	
普	執行「弱點掃描」安全檢測。

系統發展生命週期部署與維運階段	控制措施內容
高 中	一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。 二、等級「普」之所有控制措施。
普	一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統不使用預設密碼。

系統發展生命週期委外階段	控制措施內容
高	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。
中	
普	

		控制措施內容
獲得程序	高	開發、測試及正式作業環境應為區隔。
	中	
	普	無要求。

系統文件	控制措施內容
高 中 普	應儲存與管理系統發展生命週期之相關文件。

構面六
系統與通訊保護2項

傳輸之機密性與完整性	控制措施內容
高	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證應定期更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。
中	無要求
普	無要求

		控制措施內容
資料儲存安全	高	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。
	中	無要求
	普	無要求

構面七
系統與資訊完整性3項

		控制措施內容
漏洞修復	高 中	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。
	普	系統之漏洞修復應測試有效性及潛在影響，並定期更新。

資通系統監控	控制措施內容
高	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。
中	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。
普	發現資通系統有被入侵跡象時，應通報機關特定人員。

軟體及資訊完整性	控制措施內容
高	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。
中	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。
普	無要求。

相信機構會成為攻擊目標

找出機構中不可承受之痛

預算永遠不足永遠買不夠

慎選能夠一起思考的廠商

核心資料與主機不要節省

復原與避免同樣原因淪陷

完善隔離遠比找內鬼重要

敬請指導

歡迎來竹銘醫院當夥伴