113年資通安全管理彙報

資訊部/ 陳柏嘉 協理

113/11/12

- 資安政策、資安組織組成
- 資通安全投入規劃
- 投入資通安全資源
- 資通安全管理方案
- 資通安全執行成果與績效

資安政策、資安組織組成

● 資訊安全政策

- 為**強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性**，以提供本公司之資訊**業務持續運作**之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，公司於112年12月以ISO/IEC 27001為資通安全管理框架制定【資訊安全手冊】，並設定願景:

  強化人員認知、避免資料外洩

  落實日常維運、確保服務可用

● 資訊安全委員會

職務	職稱	姓名
召集人	協理	陳柏嘉
委員	總經理	李進昌
委員	財務總部 副總	羅永勵
委員	研發中心 副總	何進芳
委員	崑山廠 資訊部 協理	賴伯宜
委員	斗六二廠 廠長	蕭壹駿
委員	總廠 廠長	蔡明亮

● 資訊安全組織

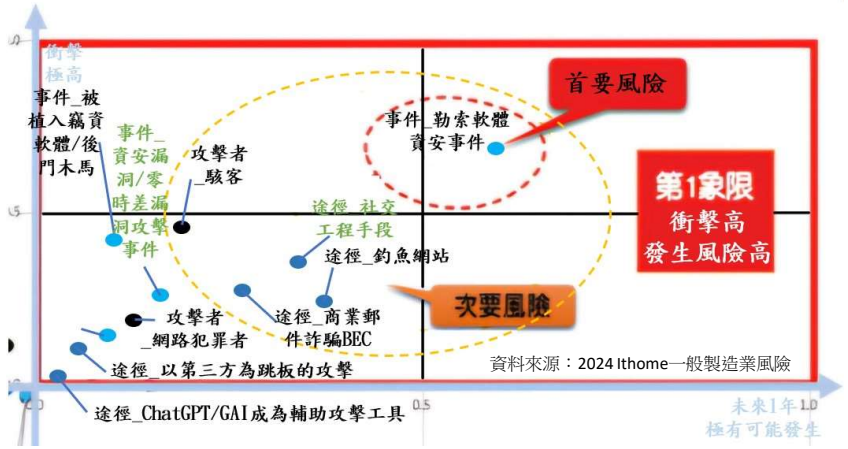
職務	職稱	姓名
管理代表	資訊部 經理	蕭相賢
資安工作小組	資訊部 副理	陳俊宇 共 17人
資安稽核組	稽核室 主任	張菁蘭 共 4人
資安應變組	資安組 課長	蕭嘉俊 共 11人

資通安全投入規畫 – 風險趨勢

- 2024 資安風險

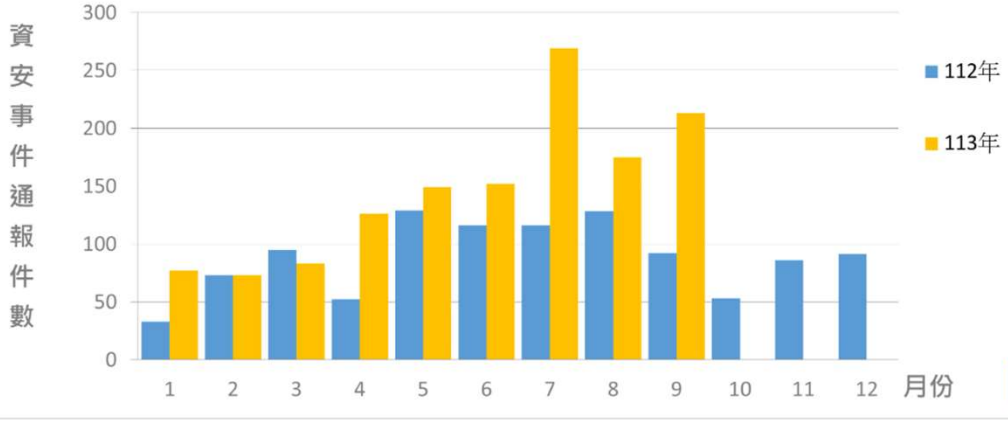
防護產品
資安教育訓練 社交工程演練
EDR、防毒軟體 oneDriver、NAS 備份 網路行為偵測
次世代防火牆 弱掃偵測、漏洞修補 情資蒐集(TWCERT)
Exchange online
次世代防火牆
微軟資訊保護、TFG 微軟MFA、條件式存取
網路行為偵測 EDR
網路行為偵測

- 2024 ~2025 一般製造業資安風險



資料來源：2024 Ithome一般製造業風險

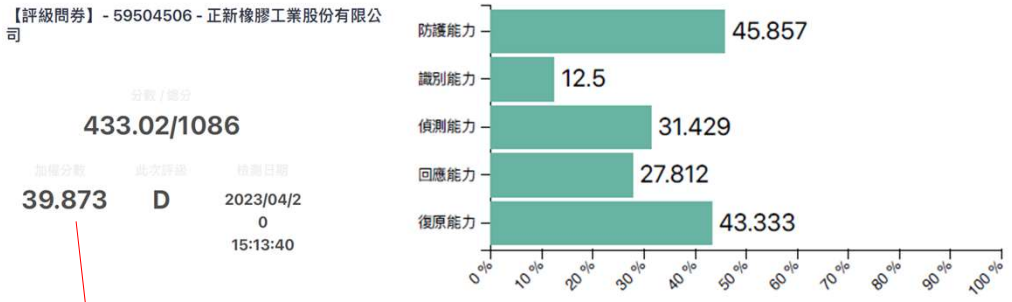
- 2023、2024 企業資安事件通報件數



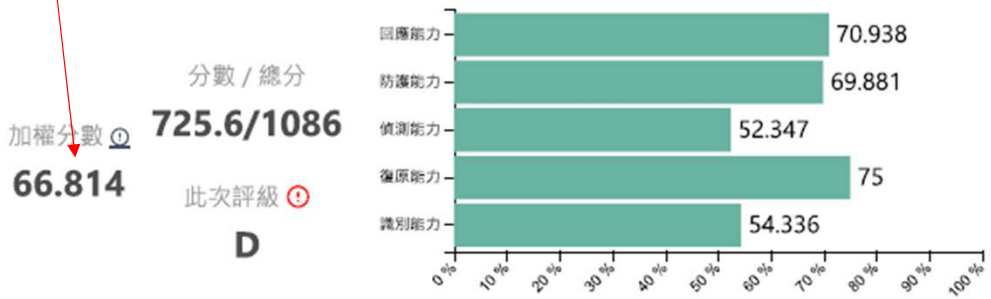
資料來源：數位發展部 113 09

資通安全投入規畫 – 內部分析

- 112年資安評級

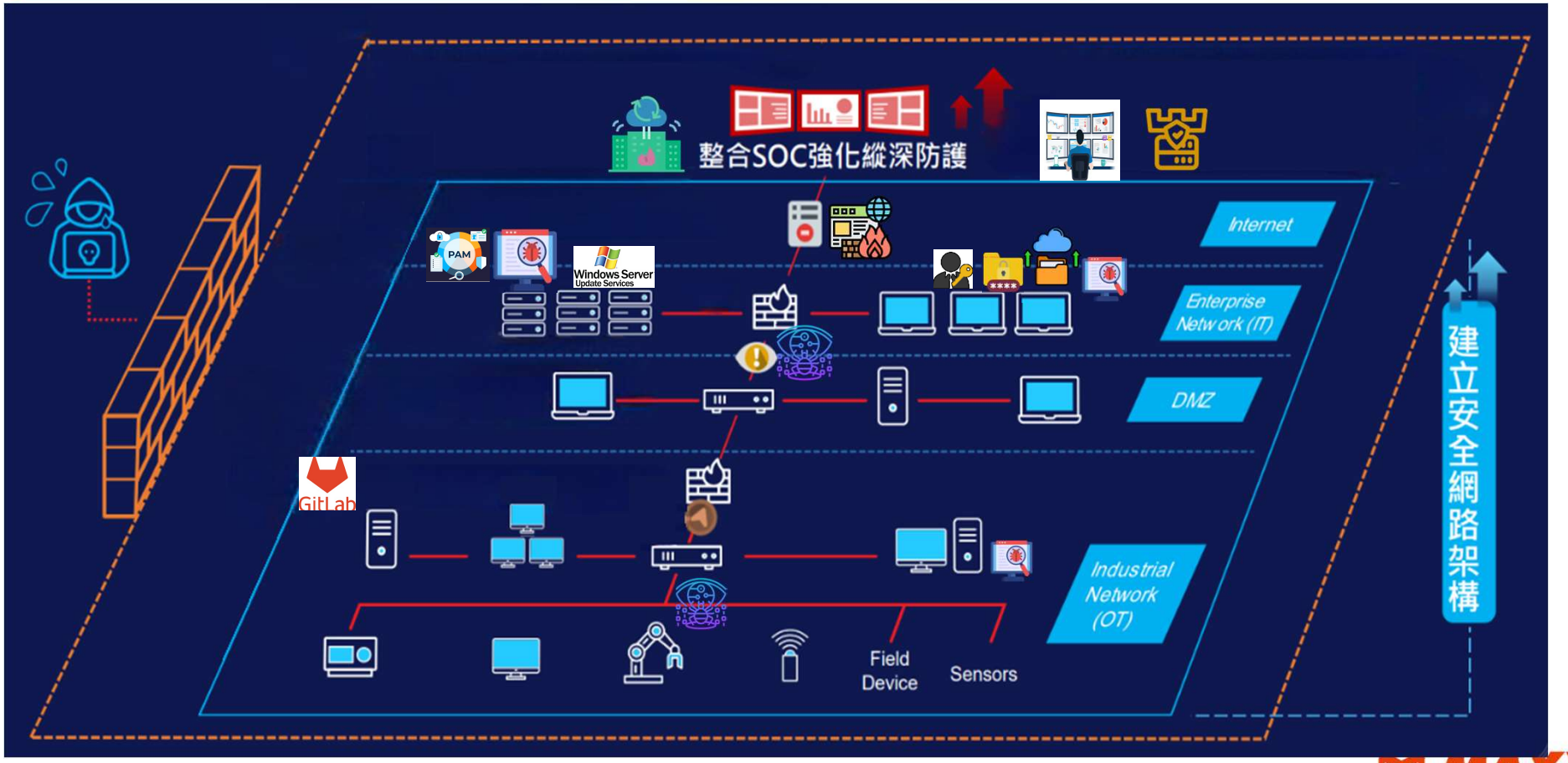


- 113年資安評級

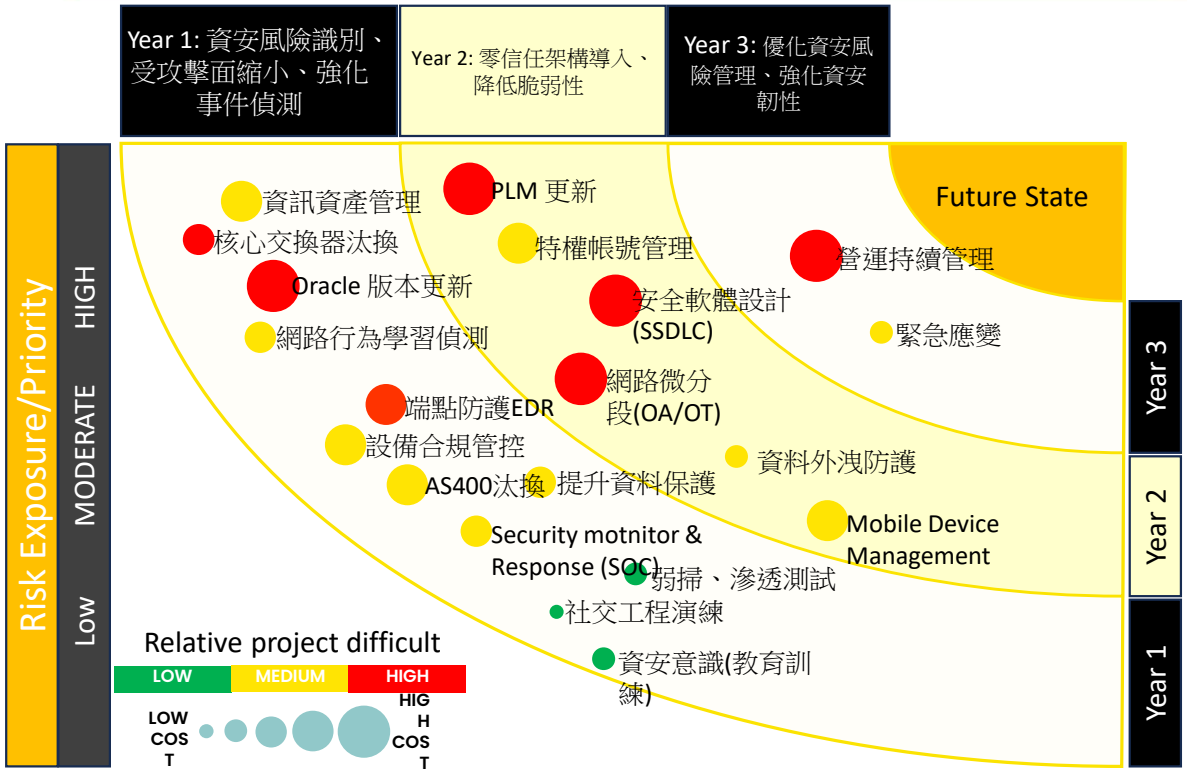


- 管理方案優化
  - Identify：特權帳號管控、弱點掃描(初 、複測、修補)、日誌保存主動告警。
  - Protect：網路微分段、條件式存取(Entra ID)。
  - Detect：內網封包行為分析搭配現有防護。
  - Respond：資安事件通報流程。
  - Recover：災難還原演練、自開發原始碼管控(gitlab)、 HCI虛擬機叢集。

資通安全投入規畫-場域部屬



資通安全投入規畫



- 114年 預計投入項目

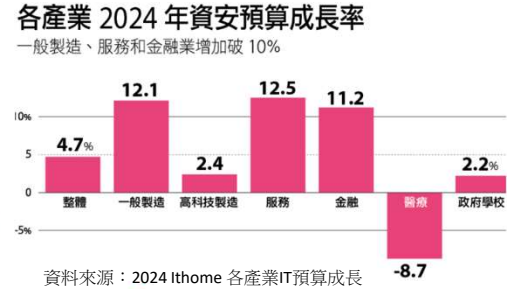
➢ ISO27001:2022、TISAX 要求項目

- ✓ 員工資訊安全教育訓練每年至少一次
- ✓ 資訊人員教育訓練
- ✓ 資安事件通報流程建立
- ✓ 特權帳號管控(數發部補助案)
- ✓ 資安演練-社交工程釣魚郵件演練 2次/1年
- ✓ 弱掃、漏洞修補 -核心系統、設備 (365合約已包含)
- ✓ MES 測試環境建置、災難還原演練
- ✓ OA、OT網路隔離 (數發部補助案)

➢ 資通安全強化

- ✓ 總廠核心交換器老舊更換 (數發部補助案)
- ✓ 核心系統/設備日誌保存 (數發部補助案)
- ✓ SAP 安全加固 (2023、2024、2025)
- ✓ PLM 版本更新、安全升級
- ✓ Oracle 資料庫版本升級

資料來源：2024 Ithome 資安預算占IT預算比



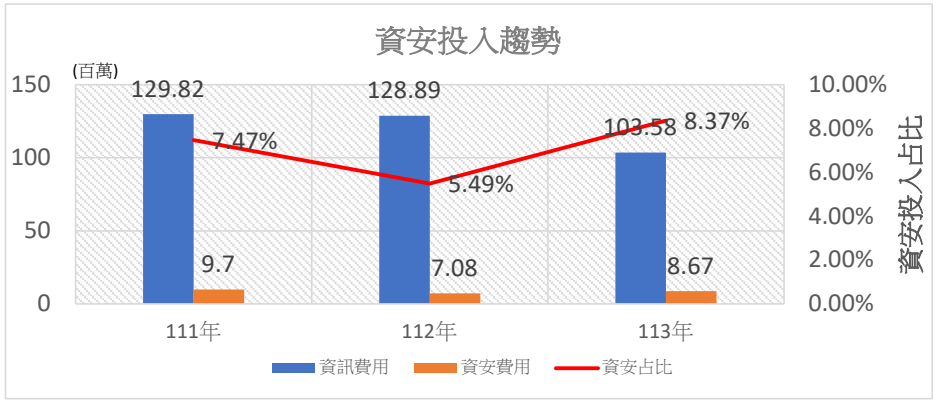
資料來源：2024 Ithome 各產業IT預算成長

投入資通安全資源

- 111~114 投入資通安全費用

資通安全範圍	項目	投資改善細項	111 年	112 年	113年	114年
1. 辨識 (Identify)	弱掃/滲透測試	1.1 資訊系統/設備弱點掃描	9,709,779	7,084,461	8,667,961	10,547,161
	身分識別	1.2 特權帳號管理				
2. 保護 (Protect)	端點防護	2-1 防毒中控系統				
		2-2 虛擬修補				
		2-3 M365 Security				
	OA/OT 隔離	2-4 網路微分段				
	漏洞修補	2-5 SAP ERP DB/PO 版本老舊升級計畫				
		2-6 SAP 安全加固服務				
3. 偵測 (Detect)	AI入侵偵測	3-1 主動防護系統				
4. 回應 (Respond)	資安威脅偵測管理 (SOC)	4-1 7*24 SOC 告警				
5. 復原 (Recover)	SAP 災難備援	5-1 SAP ERP 資料備份(IDC)				
		5-2 SAP ERP 雲端災備機制				
1-5 小計			9,709,779	7,084,461	8,667,961	10,547,161

資通安全範圍	項目	投資改善細項	111 年	112 年	113年	114年
6. 其他 (Other)	版本升級	6-1 合併財務報表 版本老舊升級計畫	52,227,156	47,539,789	41,258,200	49,566,466
		6-2 SAP VM 升級				
		6-3 PLM 升級				
	降低脆弱性	6-3 核心交換器更新				
	SAP 維護合約	6-4 SAP 維護合約(含版本更新) 及雲端產品訂閱				
	PLM 維護合約	6-5 CST ENOVIA PLM 系統軟體服務				
		6-6 CSTC PLM系統軟體服務				
小計(6.小計)			52,227,156	47,539,789	41,258,200	49,566,466
合計			61,936,935	5,4624,250	49,926,161	60,113,627

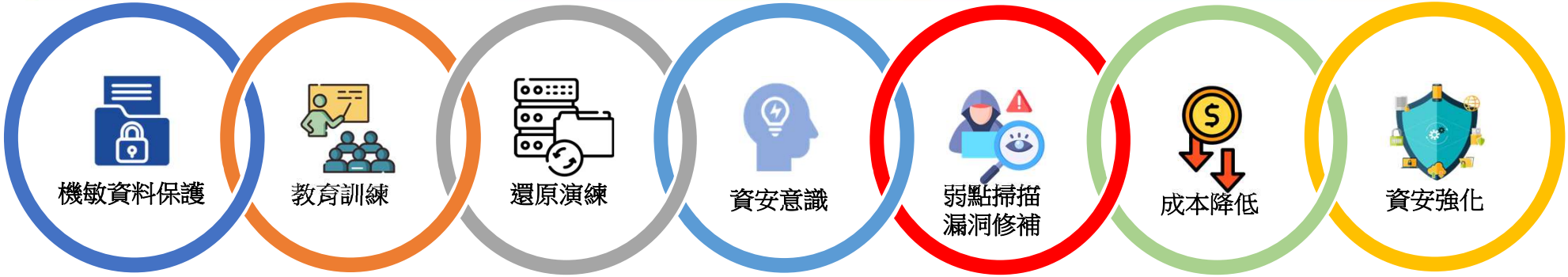


資通安全管理方案

- 具體管理方案(NIST CSF 2.0 圖)

功能	類別	方案說明	
identify	• 資訊設備識別 • 人員識別 • 風險識別 • 威脅情資管理	• 設備合規性(微軟 MAM) • 導入啟用多因素驗證(MFA) • Windows Defender 識別設備或存取風險，自動停用高風險帳號。	• 加入TWCERT/CC、Hitcon Zeroday 取得威脅情資 • 資訊設備、系統弱點掃描
Protect	• 內/外存取管控 • 資料外洩防護 • 端點防護 • 使用者上網控管	• 防火牆設定連線規則 (需申請開放) • 遠端連入內部系統需透過雲端跳板機 • 檔案加密、敏感度標籤套用、啟用條件式存取 • 安裝防毒軟體，並自動更新病毒碼	• 建立WSUS，派送微軟patch、漏洞更新 • 過濾使用者上網可能連結到有惡意程式的網站 • 建立LAPS 回收本機Administrator 密碼
Detect	• 郵件安全管控 • 內部網路封包偵測	• 自動郵件掃描威脅防護，防範惡意附件、釣魚郵件、垃圾郵件 • 內網封包行為分析、防止東西向擴散	
Respond	• 高風險行為告警 • 資安事件通報	• 7*24 SOC 資安告警通告 • Microsoft Defender 高風險行為主動告警。 • 資安事件通報流程	
Recover	• 資料、系統備份機制 • 原始碼版控、備份 • 災難還原演練 • RTO提升	• 重要系統、資料庫每日備份並於異地保留一份 • 個人資料自動備份雲端備份 • 自開發原始碼管控(gitlab)	• 核心網路設備切換演練(每年一次) • SAP 雲端 DR 切換演練 (每年一次) • 超融合虛擬機叢集(總廠、斗六)
Govern	• 取得國際認證 • 資安教育訓練 • 資安意識提升	• ISO27001:2022、TISAX AL2 合規 • 資安教育訓練 (全體員工、資訊人員→ 每年一次) • 集團資訊安全會議(雙周會)	• 不定期 Teams 資安內、外部案例 • 每年2次社交工程演練。

113 資通安全執行成果與績效



員工簽屬保密協議
合作廠商簽屬保密協議
敏感度標籤派送

全廠資安教育訓練(2HR)
實體912人
線上867人
單一重點教材 1653人
資訊人員資安教育訓練
(44人 *2HR)

核心網路設備災難還原演練*1次
SAP DR 切換演練 * 1次
AS400主備切換演練*1次

社交工程演練 * 1次
資安宣導 * 4 則
集團資安會議 : 15場

完成弱點掃描(委外)
威脅情資管理(Teams)

資安投資抵減
數發部資安零補助案

ISO27001:2022 認證取得
TISAX AL2 驗證通過
資安事件通報流程建立
停用外部VPN連線
USB 抽取式媒體管控
堡壘機導入: 維運人員多重驗證

資安指標	作業不慎、未依規定操作影響營運事件	外部入侵、資料外洩或病毒加密事件	資訊系統異常或設備異常影響營運事件	天然災害、重大突發事故
113年事件統計(件)	0	1	0	0