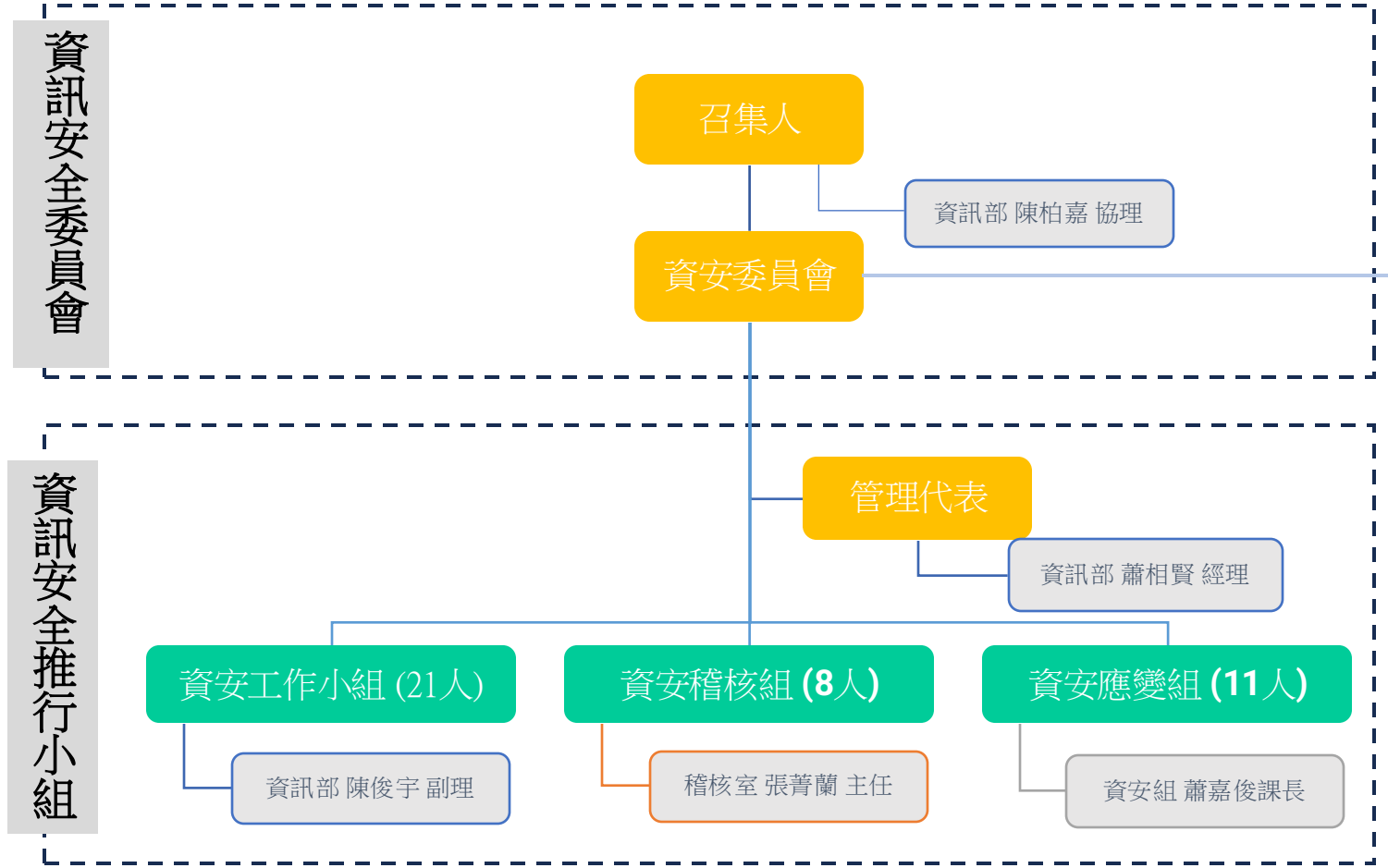
114年資通安全管理彙報

資訊部/ 陳柏嘉 協理

2025/11/12

資安政策、資安組織組成

- 公司於112年12月以ISO27001 PDCA循環及美國CSF網路安全框架的五大構面(識別、保護、偵測、回應與復原)，透過現況了解及風險評估，開始導入資訊安全管理制度，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**』



姓名	職稱
李進昌	總經理
羅永勵	財務總部 副總
何進芳	研發中心 副總
賴伯宜	崑山廠 資訊部 協理
蕭壹駿	斗六廠 廠長
蔡明亮	總廠 廠長

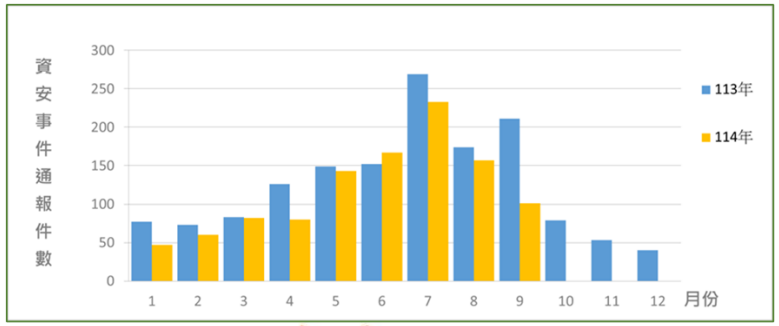
資通安全投入規畫 – 風險趨勢

2025 資安威脅	因應措施		
	事前	事中	事後
惡意勒索軟體仍為主要資安威脅且網域AD 將成為主流攻擊目標， 持續對營運造成高風險威脅	➢ 定期盤點與修正 AD 權限設定（最小權限原則） ➢ 強制多因素驗證（MFA） ➢ 部署 EDR ➢ 定期弱點掃描與滲透測試 ➢ 員工資安教育訓練 ➢ 網路微分段	➢ 7x24 監控 AD 行為 ➢ 即時偵測異常（如大量密碼查詢、權限提升行為） ➢ 啟動資安事件通報與應變流程	➢ 啟動備份還原（確保備份未受感染） ➢ 事件鑑識與根因分析 ➢ 修補遭利用的漏洞與設定 ➢ 密碼全面重設 ➢ 優化應變流程
AI 驅動的新型攻擊，加速攻擊速度和精準度，防禦難度指數級上升	➢ 加強身分驗證與行為異常監控 ➢ 員工意識培訓與 AI 使用政策 ➢ AI 治理框架	➢ 利用 AI 進行自動風險分析，預測新興威脅 ➢ 即時威脅情資共享	➢ 強化復原能力 ➢ 利用AI技術對攻擊事件進行根本原因分析
個人資料或營業祕密外洩	➢ 盤點與分級敏感資料 ➢ 進行外洩商業衝擊分析，找出資料擁有者 ➢ 制定與落實保密合約、切結書 ➢ 實施資料分級標籤 ➢ 員工資安教育訓練	➢ 立即啟動應變計畫 ➢ 控制影響範圍(隔離受影響系統並中斷惡意連線) ➢ 初步調查與蒐證	➢ 損害評估與調查 ➢ 釐清原因與責任 ➢ 依規定通報主管機關

- 2025 一般製造業資安風險

資料來源: Ithome 2025 CIO & CISO 大調查，2025年

- 2024、2025 企業資安事件通報件數

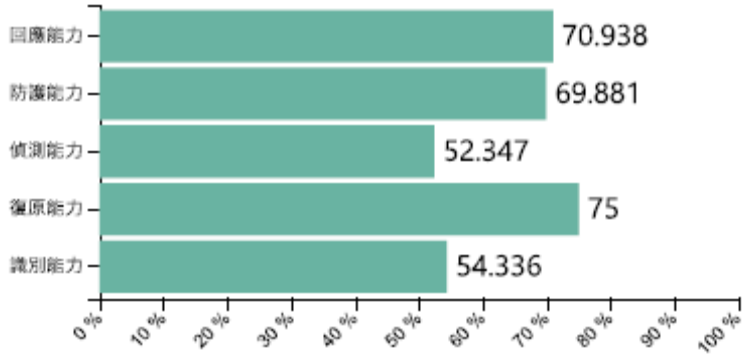


資料來源:數位發展部資通安全署資通安全網路月報（114年9月）

資通安全投入規畫 – 總廠

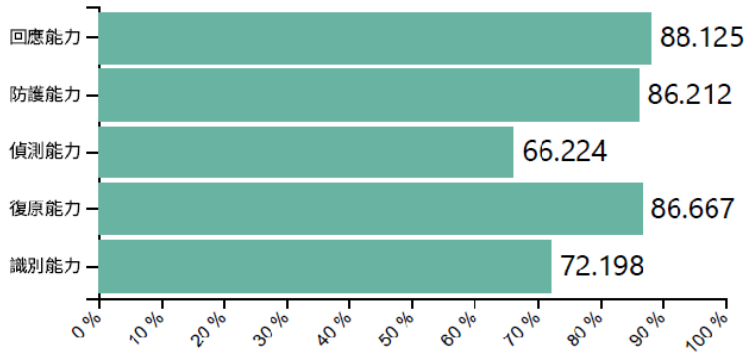
- 2024年資安評級

分數 / 總分
725.6/1086
加權分數
66.814
此次評級
D



- 2025年資安評級

分數 / 總分
901.75/1086
加權分數
83.034
此次評級
B



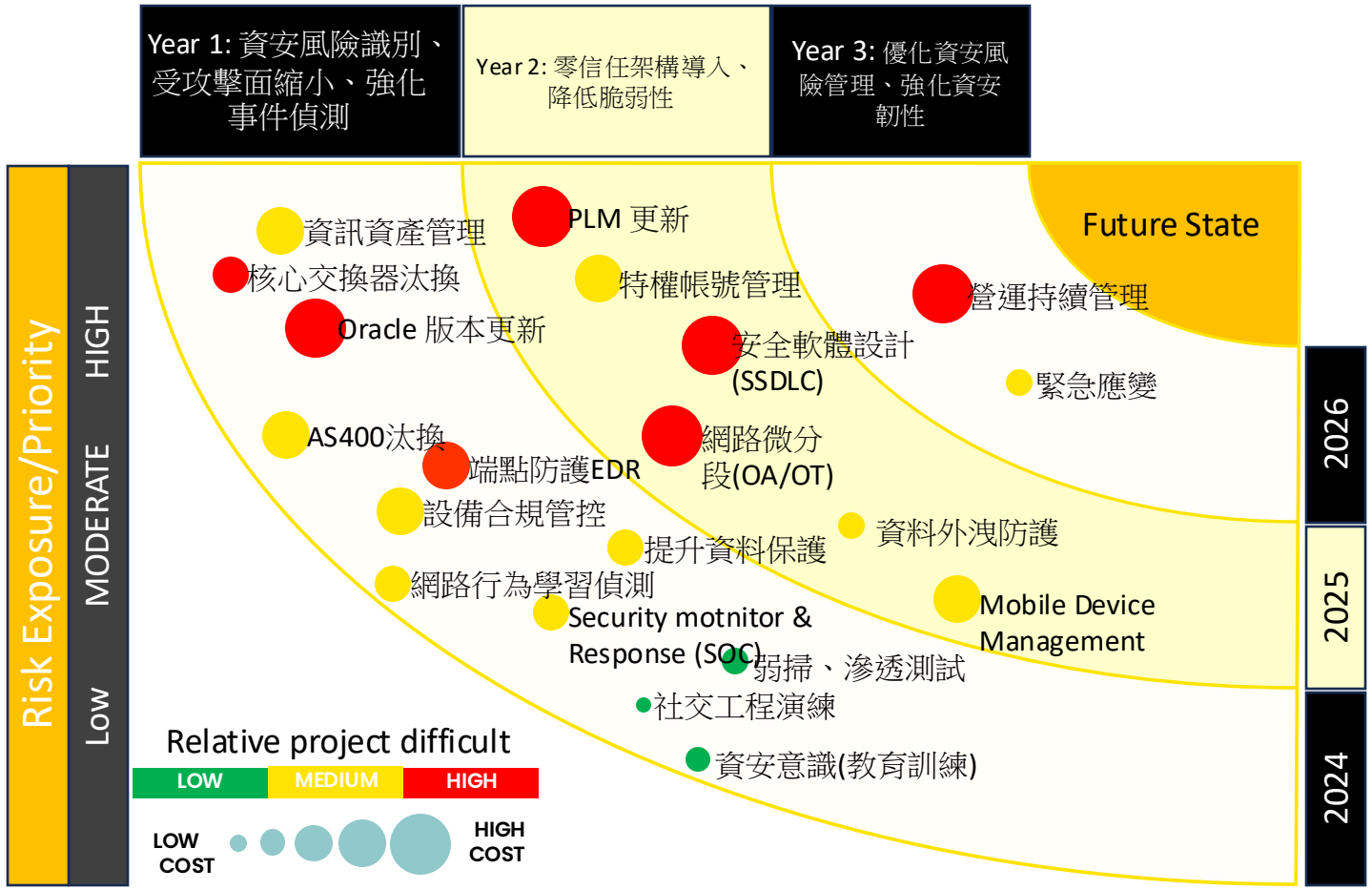
- CDM盤點內部資通安全佈署

	治理 Govern ISO27001 取證				
	Identify	Protect	Detect	Respond	Recover
Device	弱點掃描 / 威脅情資 / 設備識別	端點防護 弱點修補 虛擬修補	設備行為管控 設備狀態監視	設備異常告警	機房改善 災難還原演練 / 營運持續演練
Application	軟體清單	遠距作業管控	核心日誌分析	事件告警	原始碼版控、備份
Networks	設備接入管控 網路封包分析	邊界防護 OA/OT隔離	網路流量分析 入侵偵測	SOC 7*24 通報 惡意連線阻斷	核心網路主備
Data	機敏資料分級	資料加密	資料外洩偵測		資料備份/還原
Users	USER帳號風險評估 MFA 驗證 資安意識教育/社交工程	條件式存取 Local admin回收 特權帳號管控	異常行為偵測	資安事件通報流程 資安事故演練	

※ 🟢 - 2025 年已完成　🟡 - 2026年改善目標

- 管理方案優化
  - Identify：軟體清單控管、資安意識教育(個資保護)。
  - Protect：OA/OT微分段(混練)、特權帳號管理。
  - Detect：核心日誌主動式告警。
  - Respond：網路行為分析與回應(設備聯防)。
  - Recover：營運持續演練、超融合 虛擬機叢集。

資通安全投入規畫



- 2026年 預計投入項目

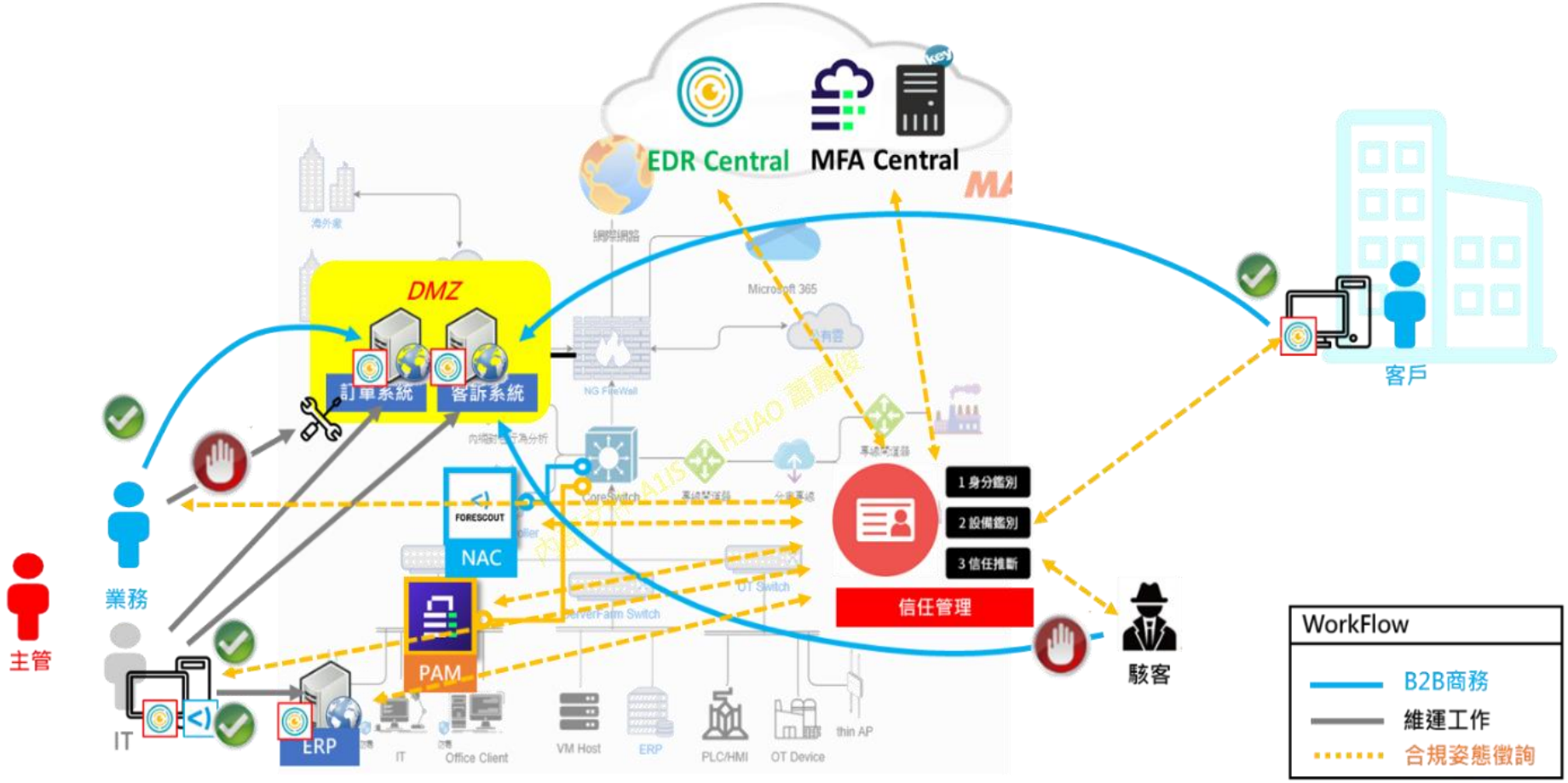
➢ ISO27001:2022、TISAX 要求項目
- ✓ 員工資訊安全教育訓練每年至少一次
- ✓ 資訊人員專業資安教育訓練
- ✓ 資安事件通報流程改善
- ✓ 特權帳號管控 (方案成本改善)
- ✓ 資安演練-社交工程釣魚郵件演練 2次/1年
- ✓ 弱掃、漏洞修補 -核心系統、設備 (365合約已包含)

➢ 資通安全強化
- ✓ OA、OT 網路隔離優化
- ✓ 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
- ✓ AS400 汰換 (人資系統更新)

➢ 營運持續
- ✓ SAP硬體汰換
- ✓ 資訊機房汰換

資料來源: Ithome 2025 CIO & CISO 大調查，2025年

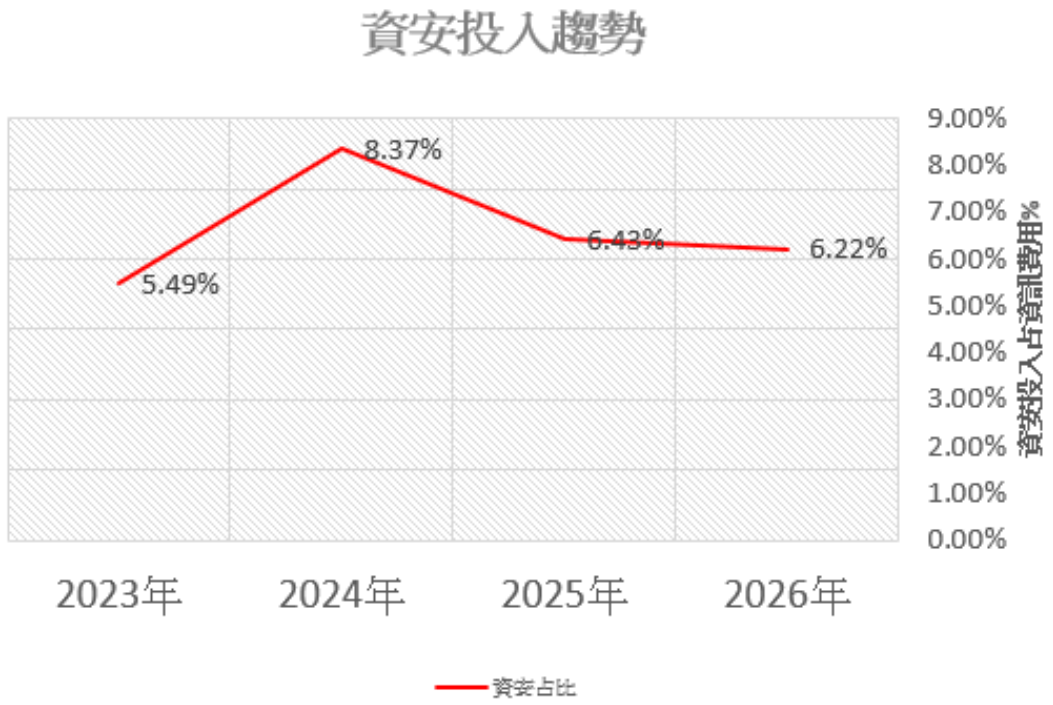
零信任架構導入- 經銷商下單系統



投入資通安全資源

- 112~115 投入資通安全費用

資通安全範圍	項目	投資改善細項	112 年	113年	114年	115年
1. 辨識 (Identify)	弱掃/滲透測試	1.1 資訊系統/設備弱點掃描	0	225,000	1,625,000	1,625,000
	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/虛擬修補	4,574,500	4,373,150	6,637,200	8,127,200
		2-2 M365 Security				
	OA/OT 隔離	2-4 網路微分段				
	漏洞修補	2-5 SAP 安全加固服務				
		2-6 SAP VM 升級				
3. 偵測 (Detect)	AI入侵偵測	3-1 網路封包分析主動防護	1,920,000	1,920,000	1,920,000	2,376,000
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 雲端災備機制	589,961	589,961	589,961	589,961
1-5 小計			7,084,461	7,108,111	10,772,161	12,718,161



※114年 網路微分段、特權帳號管控包含於數發部零信任專案。

資通安全管理方案

治理 Govern
- 取得國際認證 (ISO27001、TISAX)
- 資安教育訓練(每年2HR)
- 資安意識提升

識別 Identify
- 導入多因素驗證(MFA)
- 軟體、硬體資產管理
- 自動停用高風險帳號
- 加入TWCERT/CC、Hitcon Zeroday 威脅情資管理
- 資訊設備、系統弱點掃描
- 社交工程演練

防護 Protect
- 次世代防火牆
- 遠端作業管控 (AzureVirtualDesktop)
- 資料保護、資料外洩防護(TFG、微軟敏感度標籤套用)
- 啟用條件式存取
- EDR 端點防護
- 建立LAPS 回收本機Administrator 密碼
- WSUS 系統補丁
- OA / OT 隔離

偵測 Detect / 回應 Response
- 郵件安全管控
- AI 網路封包行為分析
- 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

復原 Recover
- 資料、系統備份機制 (321原則)
- 虛擬機叢集高可用架構
- 原始碼版控、備份 (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)
- RTO提升
- 資安事故演練

MAXXIS

資通安全執行成果與績效

2025年各項資安工作成果

管理程序修訂
8項
資安管理規定與
程序增修訂

外部稽核(每年)
2次
通過 ISO27001 認證
PWC 電腦審計

演練(每年至少1次)
2次/1Y
電子郵件社交工程演練

1次/1Y
營運持續演練(核心網路)

2次/1Y
SAP DR切換演練

弱點掃描
1次/1Y
每年1次委託外部專業廠商執行核心服務/設備弱點掃描診斷

資安管理目標
100%
設定之資安管理目標達成率

資安補助申請
1,200萬
資安投資抵減
數發部零信任補助案

重大資安事件
0次
未發生
重大資安事件

資安意識 / 資安強化
2hr/1Y
資安教育訓練

18次
集團資安會議

26件
資安威脅情資宣導、通知

1項
供應鏈資安導入零信任架構

資安防護成效

1132

網路異常行為阻斷

透過AI 網路封包分析
與防火牆聯防機制將
高風險行為自動阻斷

255

SOC 7*24 告警

針對高風險事件分析
並主動告警管理人員

5/255
(事件/告警)

高風險異常行為

使用非合規軟體、連線高風險
網址、大範圍網路掃描、大量
下載文件

24/134

異常登入

不熟悉登入、大量登入失敗、
非信任區域登入

26

惡意軟件

端點防護偵測裝置內
存在惡意軟件

50/1000
(每日)

郵件防護

惡意程式碼 / 釣魚郵件

報告結束　謝謝聆聽