

2022 資訊系統安全風險管理執行報告

Presenter: Perkins, Director

July 28, 2022



全年概況

- 資訊技術和資訊基礎架構進行優化改善
 - 與台達 Infra 進行接軌
 - ISO27001 驗證調整
- 建立資訊安全政策和基礎規範
 - 進行 ISO 27001 認證
 - 完成 IEC 62443 白皮書
 - RD實作已完成，經台達資安團隊測試 90% 符合
 - 但 RD須補安全開發規範、預計明年進行 62443 認證
- 保障重要資訊資產和設備安全
 - 168 發電機建置
 - 非認證設備不得連網



2022 挑戰

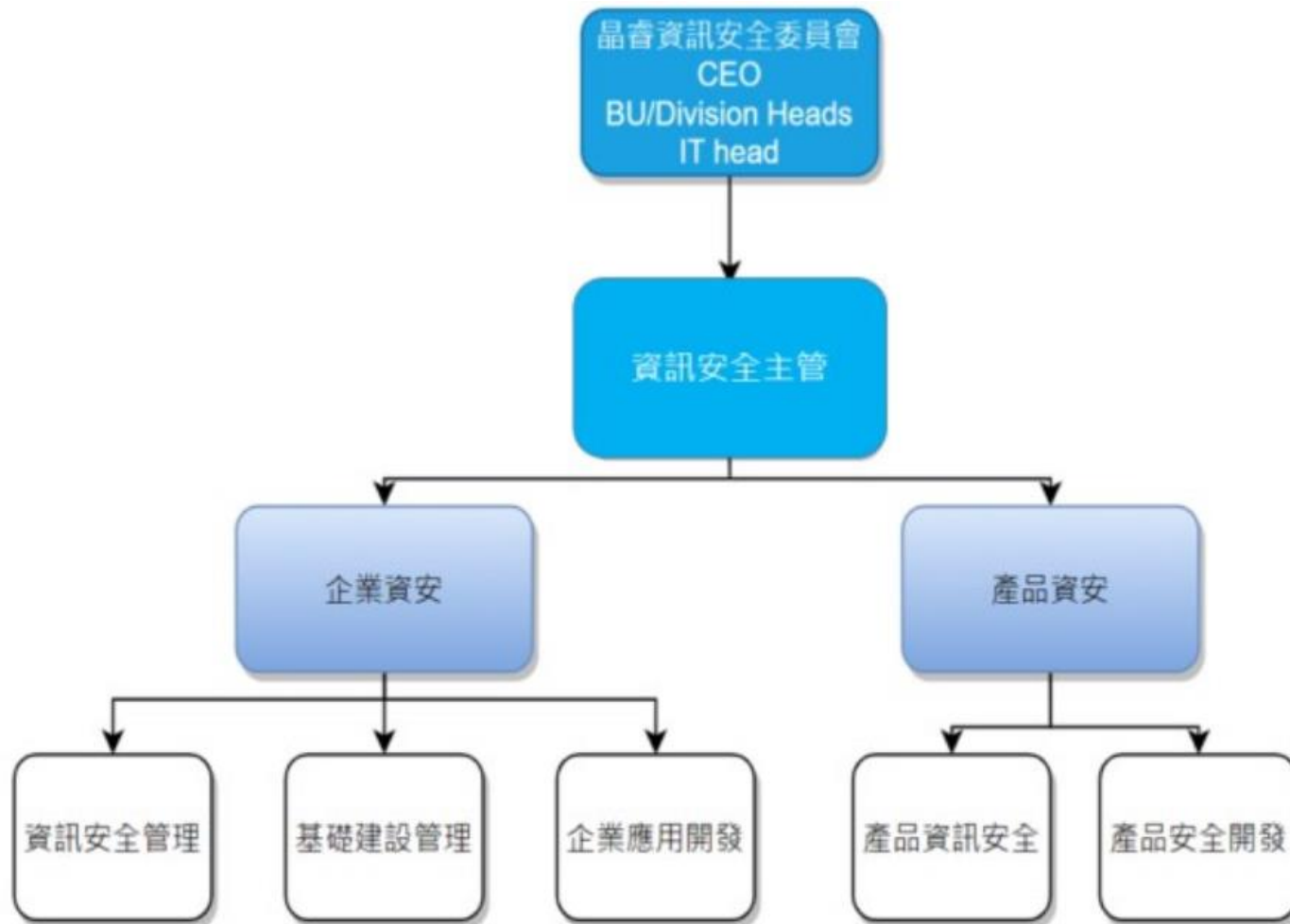
- 外部攻擊
 - 網站漏洞
 - 有兩件中度安全漏洞，因為不易被利用，目前持續觀察中
 - 帳號攻擊
 - 持續有帳號被鎖問題，請簡單型高風險帳號改帳號名稱
- 基礎建設
 - 全國性大停電
 - 夏季停電問題可能會更嚴重，建置 server 端保護機制中
 - 台達網路整合
 - 攻擊可能來自內部，須做好零信任準備
 - 整合需要人力排擠內部防護工作較不急項目 – 如測試網路規畫整理
 - 全球性內部服務可用性
 - VPN 連回總部速度受限 – 雲端系統使用可緩解此問題


資訊系統安全策略

- 強化資訊安全組織

- 晶睿資訊安全委員會於 2020 年 1 月正式成立，主委由總經理擔任，委員則由各單位一級主管擔綱。主要任務為資訊安全政策制定、資訊安全維護、資訊安全架構制定、系統弱點掃描、產品資訊安全審核等。資訊安全委員會於 2021 年設有資安主管及專責資安人員定期於每年 12 月舉行會議，檢討資訊策略，與當年資安執行成果，並制定下個年度的資安工作要點，再交由資訊安全團隊實現目標。

- 本報告已經於 2022/7/27 於董事會進行簡報完成





資訊系統安全政策

- 資訊安全政策
 - 「確保業務資訊安全、保障業務持續營運」
 - 適用於所有同仁、臨時契約人員、委外廠商，使用本公司資訊資產之外部組織人員
- 要求
 - 不侵犯智慧財產權
 - 不安裝和使用任何沒有適當授權的軟體或服務於業務上
 - 安裝防毒軟體
 - 資訊設備遺失盡速回報
 - 公司電子信想僅作公司業務使用
 - 未經授權允許，不可接露公司業務資訊與秘密
 - 善加保管公司資訊系統帳號密碼
 - 迅速回報任何資安事件與網安事件



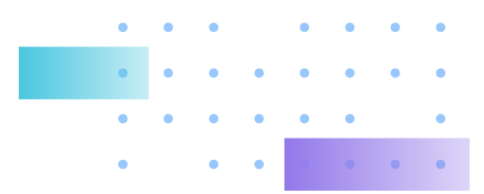
111 年度資安執行報告

- ISO27001 認證執行結果
 - 內部稽核兩次
 - 共有主缺 19 + 3
 - 次缺 11
 - 主要集中於
 - 實體問題 – 機房、環控、佈線、上網管制
 - 文件問題 – 因為換 tenant 資料未轉移完整，重新補齊
 - Server 管理 – 網路未分段、DOP 安全漏洞
 - 7/4 預稽 – 11 個建議事項
 - 文件簽核層級與規範不同
 - 7/8 第一次外稽 (線上，文件為主)
 - 兩個建議事項
- 7/18 – 第二次外稽兩個次缺，稽核建議可以發證，預計八月可拿到證書
- 8/3 拿到證書，效期 2022/7/29~2025/7/28



111 年度資安執行報告

- 投入資源
 - 資安人員一位進行規範撰寫與認證規劃
 - 兩位資訊基礎團隊成員改善網路實體環境與軟體設定
- 教育訓練
 - 全組織資訊安全教育訓練
 - 90.6% 參與現場或線上(錄影)訓練
 - 平均 每人訓練時數 0.95 hours
 - 高階董事會成員參與資安訓練
 - 八位董事會成員參與 3 小時線上課程
 - 另有 62 位其他公司成員參與訓練



111 年度資安執行報告

- 執行事項
 - eMail 整合 (升級 O365 E3)
 - DLP 佈建
 - 機房整理、理線
 - Firewall 規則整理與檢視
 - 對內與對外 Server 網路區分
 - DOP 伺服器升級
 - 插網設備需認證的設備才能聯網

- 168 機房建置發電設備，確保研發系統可安全關機
- 測試開發網路規畫調整

Thank You for Your Attention.



VIVOTEK
A Delta Group Company

We Get The Picture