CYBERSEC 2022 臺灣資安大會

NOW CHANGE

數位轉型 資安升級

國際大廠資安稽核因應策略

楊仕全

SEP. 20-22 臺北南港展覽二館

緣起

2018 年9月因中美貿易戰後，國際大廠原位於大陸生產繪圖顯示卡之生產線，無法繼續供貨美國，因而轉向撼訊科技公司採購.....

產線移回台灣。

1. 價格不得調升超過10%。
2. MIT製造出口，迴避美國課徵關高額稅。
3. 帳期延長，毛利下降。
4. 重新評估生產據點、生產設備。
5. 調整生管團隊作業。

產線留在大陸。

1. 客戶要求降價10%，彌補關稅上升後的成本。
2. 出口美國關稅由0%增加為10%。
   隔年第二季關稅提高至25%。
3. 生產基地不用改變。
4. 可能失去客戶。

面臨困境

因為稽核報告出來後真正要改變的，其實是組織與相關同仁的習慣及文化，有時這些改變是很違反人性的。如果不謹慎以對，反彈的力道往往會超乎想像。

面臨困境

為了訂單老闆肯定力挺。

資源不夠搬不了這顆石頭?

這顆石頭是公司反覆執行而且有效
讓公司活下來的累積。

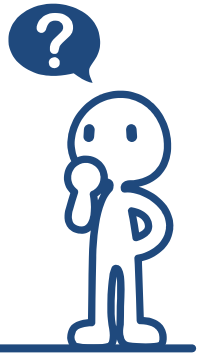
我們繼續當優良的水管工?!

必要認知

01 企業文化

02 企業價值觀

隱藏風險 03



- ✕ 因為高層不支持與資源不足所以就這樣
- ✕ 一味追求零風險的資安
- ✕ 誰支持你就要給你權力

○ 花許多時間與精力去思考，到底該拿這顆企業生存下來的大石頭怎麼辦!

善用資源

SECPAAS 資安整合服務平台 Security Platform as a Service

Search ...

熱搜關鍵字：行動資安防護 滲透測試 / 紅隊演練 風險評估 物聯網資安防護 端點安全防護

關於我們 產品服務 推動成果 最新消息 服務申請 合作夥伴 聯絡我們 會員登入 繁中

企業資安評級概述

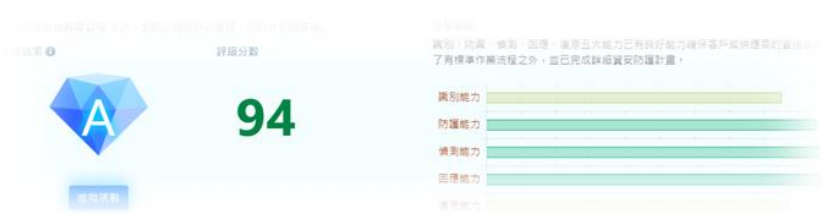
過去資安投資往往看不見成效，同時資安人員也苦於缺乏客觀依據來評估自身企業距離國際最佳實務的資安防護還差距多少。因此企業需要一種新的方法-資安成熟度評估，過去大家談到標準合規的缺點是僅能知道「有」、「無」差別，合規性並不意味著您企業是安全的，必須要清楚知道企業真實的資安成熟度才是正解。例如：在門上放一把鎖可以滿足合規性要求，但是實際上門鎖確有不同的類型，如喇叭鎖、機械鎖、天地鎖、電子鎖、防爆電子鎖等，它影響著門鎖的安全性。為了解決這些缺點，企業資安評級成為一種受歡迎且必不可少的機制

管理能力	防禦能力	偵測能力	反應能力
OT資產管理	OT系統安全	OT系統日誌	OT系統復原
OT安全組織和意識	身分與訪問控制	OT偵測安全事件	安全事件回應計畫
OT系統維護	OT系統彈性 (系統與通訊保護)	威脅分析與警報	
實體安全	OT網路安全 (系統與通訊保護)		
OT安全評估 (風險管理)	惡意程式防護 (系統與通訊保護)		
OT資安政策和流程 (風險管理)	OT資料安全		

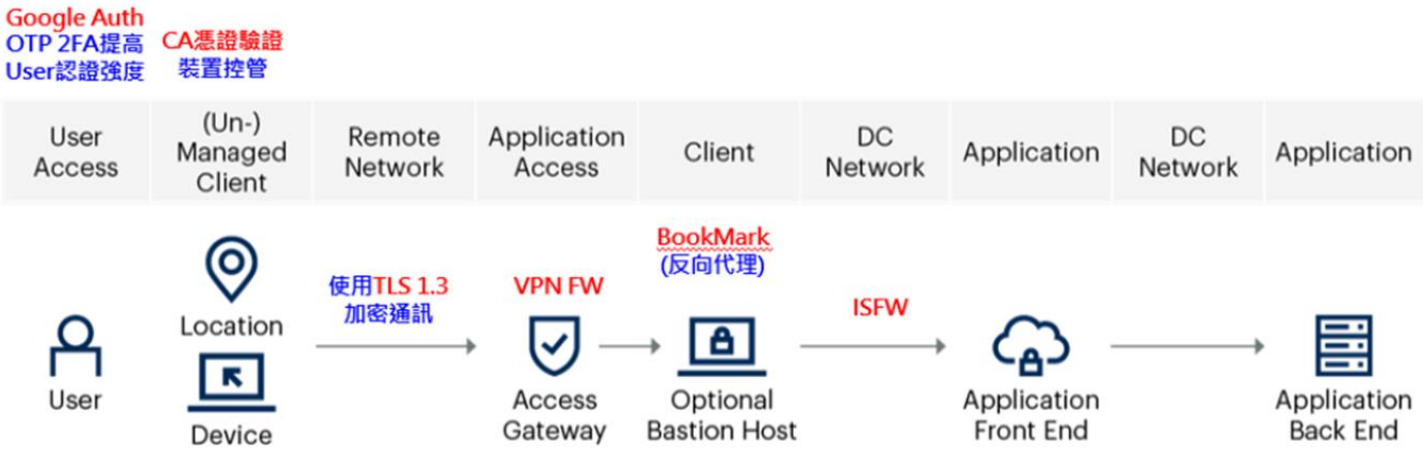
SECPAAS 資安整合服務平台 Security Platform as a Service

Security Level	質化描述
A	產線資安成熟度非常高，具備完整的制度、流程與防護措施，能夠抵禦複雜的威脅與漏洞攻擊，因此發生產線中斷機率極低，產生經濟損失可控制在極小範圍內。
B	產線資安成熟度相對高，具備良好的制度、流程與防護措施，能夠抵禦多數的威脅與漏洞攻擊，因此發生產線中斷機率相對低，產生經濟損失可控制在較小範圍內。
C	產線資安成熟度符合常規，具備尚可的制度、流程與防護措施，能夠抵禦一般的威脅與漏洞攻擊，因此發生產線中斷機率偏低，產生經濟損失可控制在一定範圍內。
D	產線資安成熟度相對低，具備基本的制度、流程與防護措施，僅能夠抵禦偶發性/常見的威脅與漏洞攻擊，因此發生產線中斷機率偏高，產生重大經濟損失的可能性相對偏高。
E	產線資安成熟度處於初始階段，僅具備入門級的制度、流程與防護措施，通常無力對抗偶發性/常見的威脅與漏洞攻擊，因此發生產線中斷機率極高，產生重大經濟損失的可能性極高。

善用資源



最小可行性



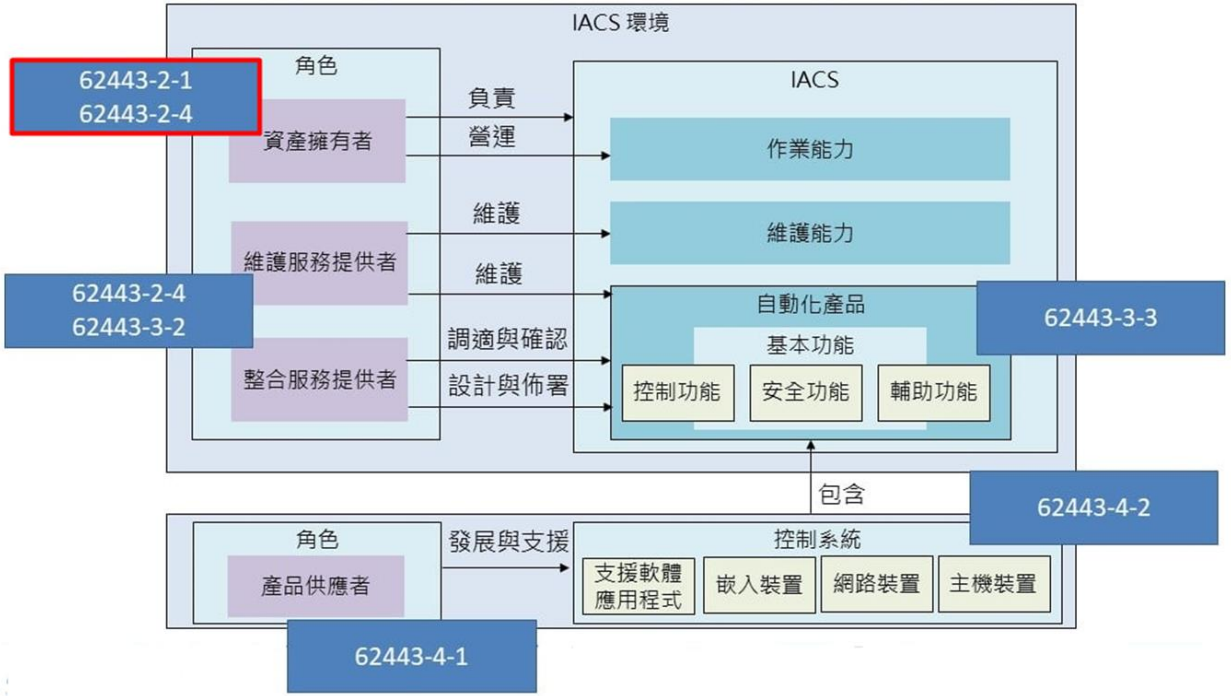
跟供應商建立安全存取流程

國際認證

ISA/IEC 62443

一般	62443-1-1 概念與模型	62443-1-2 主要用語與縮寫	62443-1-3 系統安全符合性指標	62443-1-4 安全生命週期與使用案例	
政策與程序	62443-2-1 IACS 資產擁有者安全管理制度需求	62443-2-2 IACS 保護等級	62443-2-3 IACS 環境的更新管理	62443-2-4 IACS 方案供應商需求	62443-2-5 IACS 資產管理者實作指引
技術	62443-3-1 供 IACS 的 安全技術	62443-3-2 安全風險評估與系統設計	62443-3-3 系統安全需求與安全等級		
組成	62443-4-1 產品發展需求	62443-4-2 IACS 組成之技術安全需求			

國際認證



工業自動化和控制系統安全（Industrial Automation and Control System, 簡稱IACS）

供應鏈資安管理系統機制

現階段

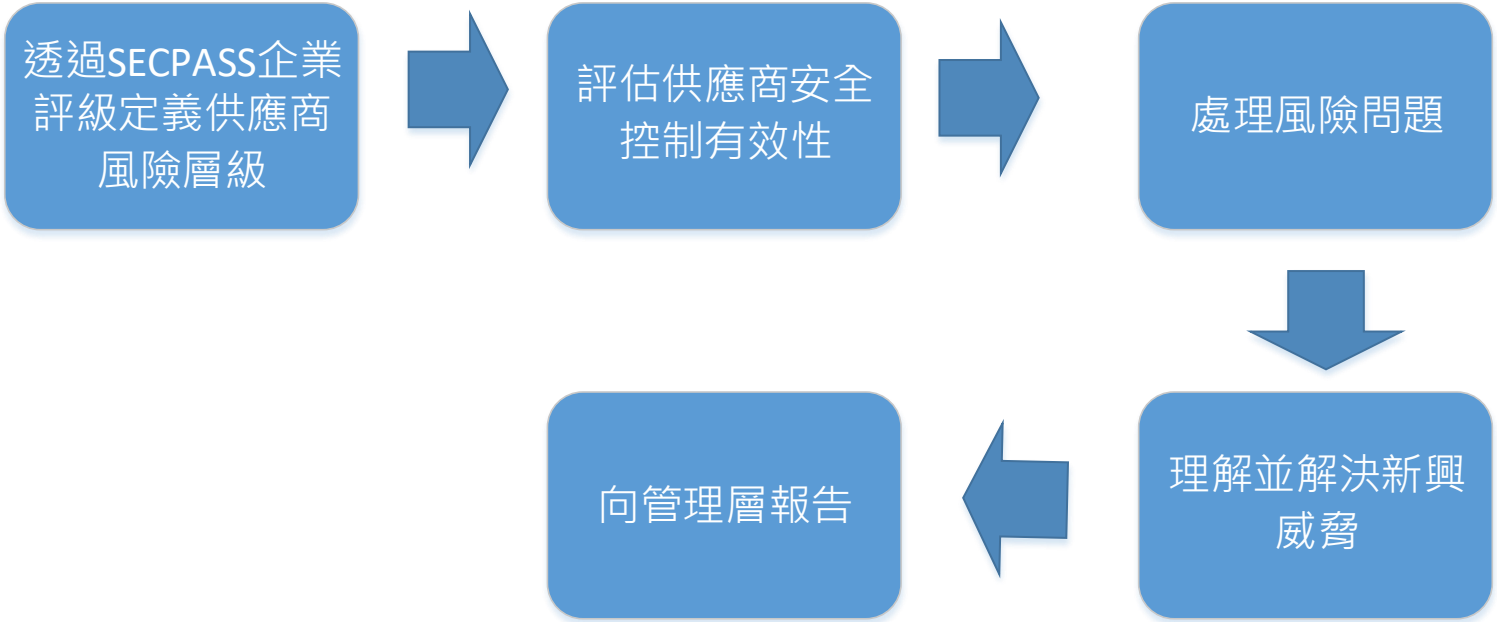
請供應商於SECPASS做企業資安評級檢視現況

依據缺口與供應商進行評估改善

建議供應商依據SECPASS防護指引進行改善

資安責任共同承擔模型SSRM（最終階段）

供應鏈風險管理機制


透過SECPASS企業評級定義供應商風險層級
評估供應商安全控制有效性
處理風險問題
理解並解決新興威脅
向管理層報告

心法

可以從不同程度去進行要求，但避免一次要求太過頭

- 盤點
- 識別
- 調整配置
- 隔離
- 保護端點
- 與既有資安管理制度整合
- 事件收集與風險分析
- 存取控制考量風險

謝謝聆聽