



資訊安全評級與提升補助計畫
經濟部工業局111年度專案計畫

產業資安強化推動工作小組(SIG)
推動說明

報告單位：台中市電腦商業同業公會
報告人：陳峰森 經理



INDUSTRIAL DEVELOPMENT BUREAU,
MINISTRY OF ECONOMIC AFFAIRS
經濟部工業局

簡報大綱





PART
01

計畫緣起

計畫緣起

- ▲ 美中科技分流下，美中政府各自制定供應鏈安全標準，**國際大廠將供應鏈資安納入企業風險評估項目**，產業也日益憂慮ICT產品與服務之供應鏈中的威脅與漏洞，開始稽核供應鏈體系資安，帶起產業資安需求。
- ▲ 經濟部工業局為提升產業資安韌性，推動ICT產品資安強固，委託工研院執行「跨域資安強化產業推動計畫」及「新興物聯網資安示範推動計畫」，**111年建立產業資安強化推動工作小組(SIG)機制**，推廣企業資安評級，設置北中南區產業服務團，委由**工研院、台中市電腦商業同業公會、成功大學產業永續發展中心**，推動產業資安SIG，希望結合產、官、學、研及法人專家，協助產業有效提升資安防護能量。

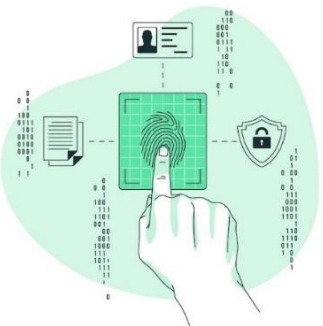


**PART
02**

推動目標及預期效益

推動目標

企業評級



- **國際大廠**對**供應鏈資安**日益重視，藉此**提升產業資安意識**、**有效評估供應鏈網路安全態勢**及**建構供應鏈的資安風險評估框架**。
- **評級工具**：本年度企業資安評級由**1.0轉化為2.0**，明確定義與銜接國內政府單位對資安的規範與標準、減少資安投入成本，讓中小型企業也能適用，帶動**資安聯防**，以因應網路安全攻擊。
- **評級輔導**：依據2021資安事件發生比率、國際大廠/法規要求急迫性與經濟衝擊，111年優先推動：**電子資訊業**、**民生工業**與**金屬機電工業**，由服務團結合**產業公協會**或**聯盟**籌組**SIG**，並導入**資安顧問輔導團**，建立實務案例、帶動合作商機與**推廣交流**。

紅隊演練



- **為強健企業內外資安防護**，**強化產業資安防護與應變機制**，在不影響企業營運的前提下，對企業進行**模擬入侵攻擊**，在有限的時間內從各種進入點執行攻擊，嘗試達成企業指定的測試任務。
- 依據2021資安事件發生比率、經濟衝擊，選出111年重點產業：**大型科技業**、**上市櫃製造業**等，**驗證資安解決方案的有效性**、理解核心系統被入侵的路徑、提升民間防護能量，有效抵禦駭客攻擊掌握高風險漏洞被利用的情況。

預期效益

- 111年推動**10個**產業SIG完成**資安藍圖規劃**，促成**150家**廠商與資安服務業者合作投入資安治理成熟度機制導入，帶動供應鏈強化資安投資，並導入**10家**紅隊演練示範案例。
- 推動企業自建或採用第三方輔導資安顧問服務，促成產業導入資安套裝解決方案，帶動資安投資與合規。



通過國際 資安稽核

協助企業提升資安成熟度，並逐步完善資安治理機制，確保供應鏈安全，**以滿足國際大廠對供應鏈資安稽核要求**



驗證企業 防護能力

落實**紅隊演練**協助企業藍隊解決重要弱點，**並驗證資安弱點**，**改善資安防護與應變機制**，建立資安韌性，且導入國產資安方案



爭取新興 產業大單

強化OT/IT資安防護，**確保企業營運安全**，爭取客戶**高毛利產品合作機會**，或避免被客戶壓縮獲利空間，有效提升企業獲利

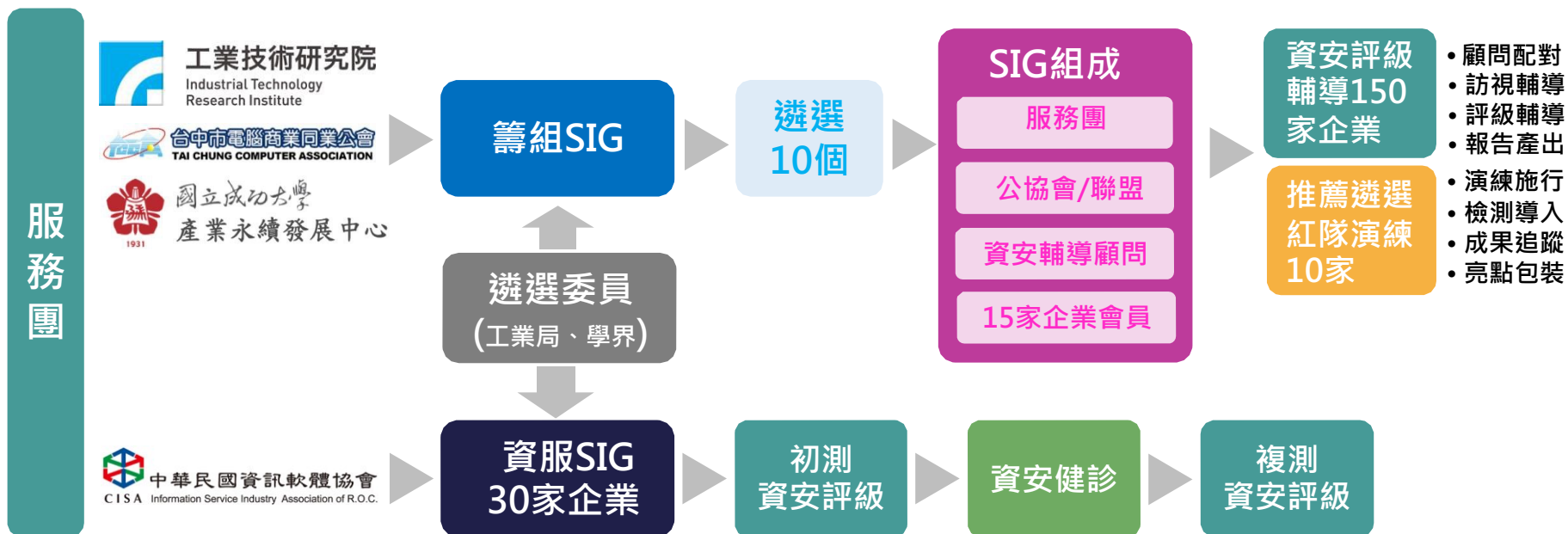


**PART
03**

計畫內容說明

產業資安強化推動說明

1. 「產業資安強化推動小組SIG」計畫執行角色

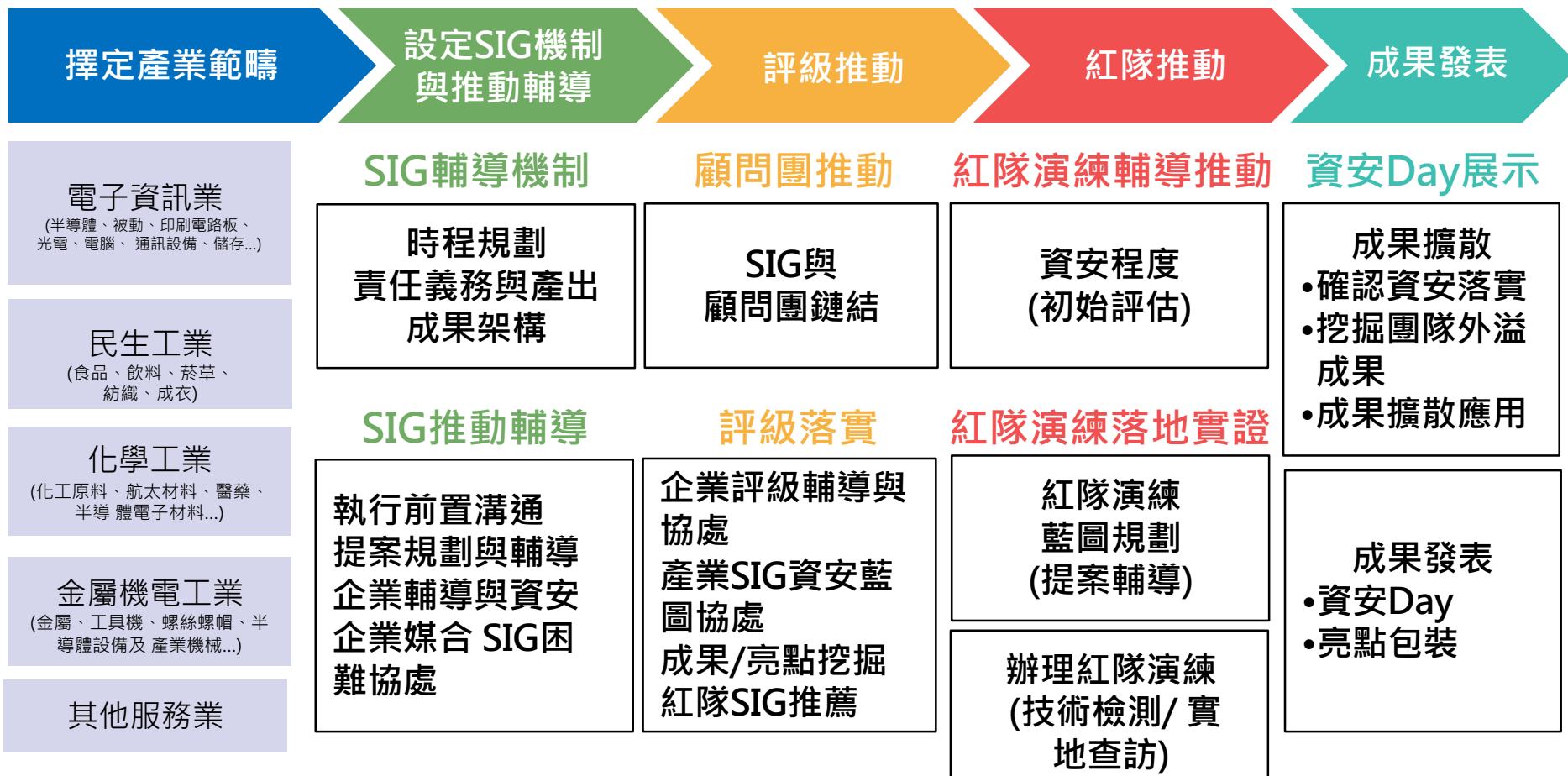


2. 計畫工作主軸說明

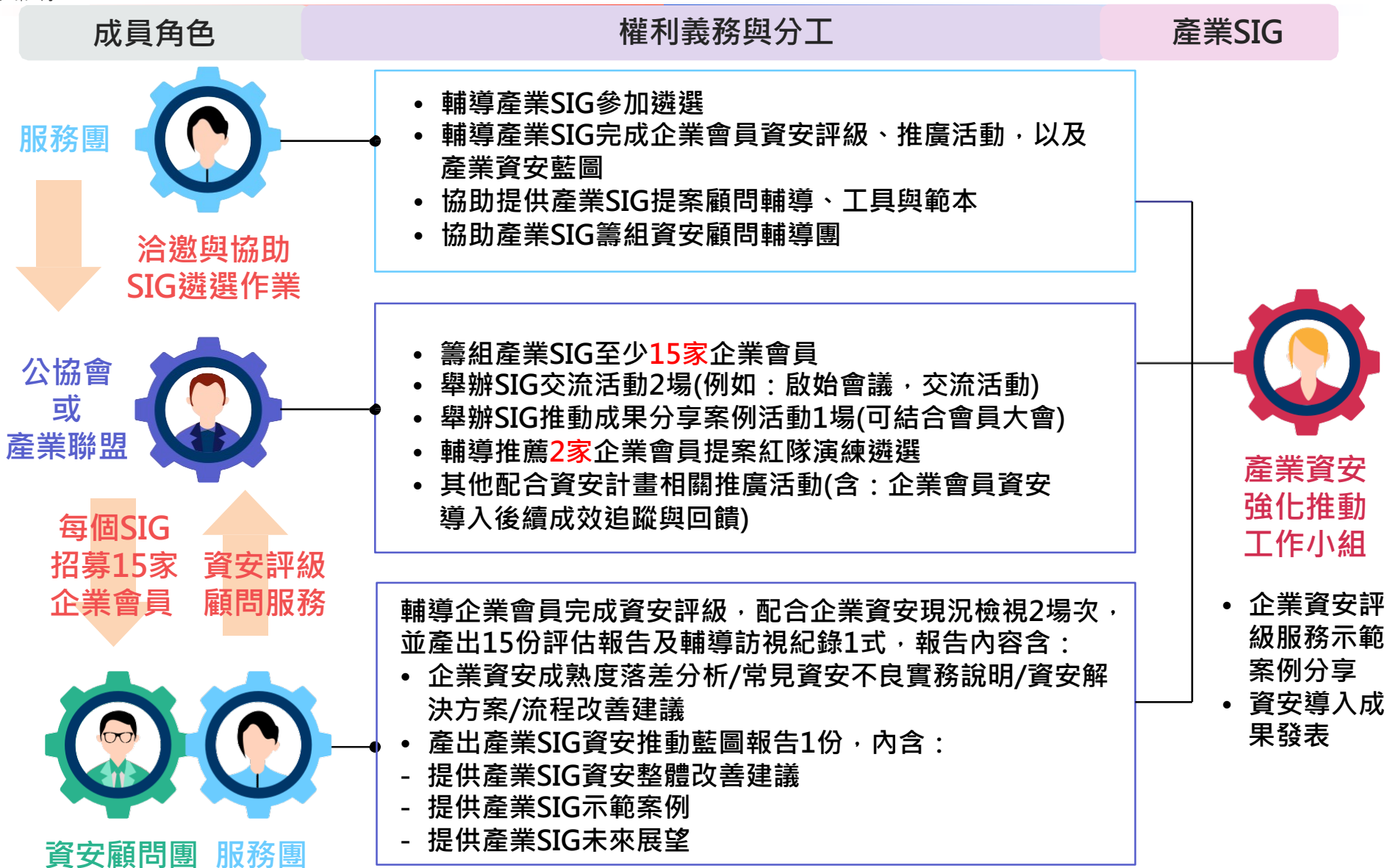
透過產業公協會(SIG)推薦會員企業完成**企業資安評級**，服務團協同資安顧問針對評級結果提出建議報告及改善方式，並邀請資安導入符合條件之會員企業申請**紅隊演練**，彙整產出**產業資安強化發展藍圖**，結合企業實證之成果，辦理**成果擴散發表**。

產業資安SIG推動架構

- 為服務北中南產業，工研院、台中市電腦商業同業公會、成大產發中心，共同籌組10至15個SIG參加遴選，帶動150家企業會員參與。
- 協助SIG企業會員完備**資安評級**、**紅隊推動**，並於輔導過程中協助**發掘亮點成果**。



產業SIG成員角色與分工



企業資安評級服務時程規劃

111年
5-6月

- 先行了解會員廠商之資安需求
- 公會偕同服務團與顧問先行線上訪談4家廠商
- 舉辦SIG啟動會議

- 企業資安評級 (15家)
- 訪視：
公司資安現況檢視
評級報告討論
方案建議導入
- 訪視時描繪產業資安藍圖
- 舉辦產業資安交流研討會

- 推薦紅隊演練廠商 (2家)
- 追蹤輔導紅隊演練廠家進度

111年
6-10月

- 產出產業SIG資安藍圖
- 舉辦SIG推動成果分享案例活動1場
- 企業資安評級服務示範案例分享擴散

111年
11-12月

產業SIG審查標準

項目	說明	內容	配分
計畫內容	資安急迫度	<ol style="list-style-type: none"> 1. 申請單位需具數位化環境 2. 問題情境與需求痛點 (如國際大廠稽核) 3. 資安技術導入目的 4. 預期產生效益(含量化與質化) 	25%
	經濟衝擊程度	<ol style="list-style-type: none"> 1. 產業背景與重要性 (如經濟貢獻度、資安急迫度) 2. 推動產業資安化對台灣經濟貢獻度，如 GDP占比、產值投資投入等 	10%
	跨域合作整備	<ol style="list-style-type: none"> 1. SIG具備代表性廠商或參與落地應用之廠商能力及號召力 2. 資安輔導顧問資格條件審查 3. SIG會員生態圈(包括系整、資安廠商、上下游供應商等)串連與合作關聯度與完整度 	25%
執行能力		<ol style="list-style-type: none"> 1. 曾參與的政府或產業推動計畫。 2. 輔導服務團隊與申請單位的合作分工模式規劃。 	15%
未來成果擴散性		<ol style="list-style-type: none"> 1. 規劃項目之可延續性及未來發展方向 2. 成果行銷推廣企劃與說明 	25%

產業SIG徵選應備文件

【6/2(四)17:00前提交】

1. 計畫申請表
2. 協會(法人)登記證(立案證明)掃描檔
3. 產業聯盟成立證明
4. 提案簡報 (簡報格式)

簡報注意事項

- 全程簡報時間以15分鐘為限
- 簡報內容以20頁 (不計算附件)為限
- 簡報標題及重點處請加粗，各頁內容盡量以圖表配合量化數字說明，並摘要重點敘述

基本資料

產業服務團	<input type="checkbox"/> 工研院 <input type="checkbox"/> 台中市電腦商業同業公會 <input type="checkbox"/> 成功大學產業永續發展中心		
申請單位	<input type="checkbox"/> 公會 <input type="checkbox"/> 產業聯盟	成立年份	
名稱			
產業類別		會員數	
通訊地址	□□□		
代表人		員工人數	
聯絡人	職稱	手機	
	電話 (00)	分機	
	Email		
資安強化 應用範圍			

一、同意事項：

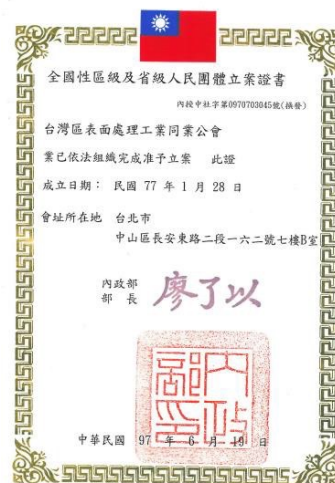
1. 同意由執行單位(產業服務團)轉請審查委員會審查本單位提出之中請資料。
2. 有義務回答審查委員會之審查意見。
3. 本簡所提供個人資料之當事人，均已瞭解並同意所提供之個人資料，將依產業資安強化推動工作小組(SIG)申請須知相關辦法之作業程序進行管理；明確若提供不正確之個人資料，執行單位即無法進行前述各項作業。

二、聲明事項：

1. 申請文件所列資料及附件均屬正確，符合申請相關規定，並保證不侵害他人之相關智慧財產權。
2. 3年內未有因執行政府科技計畫受停權處分，且其期間尚未屆滿情事。
3. 未來針對本計畫之合作成果，不得進行誇大不實之宣傳。
4. 申請文件所提供之各項資料，均與申請單位事實相符，並保證報載資料正確無誤，否則願負一切責任。
5. 申請單位負責人未具有大陸地區人民來臺投資許可辦法第三條所稱之投資人身分，(「大陸地區人民來臺投資許可辦法」第三條所稱投資人，指大陸地區人民、法人、團體、其他機構或其於第三地區投資之公司，依規定在臺灣地區從事投資行為者。)」以上所提供之各項資料，均與申請單位事實相符，並保證報載資料正確無誤，否則願負一切責任。

(請加蓋申請單位印鑑及負責人印章)

申請單位印鑑： 負責人簽字：





**PART
04**

企業資安評級說明

推動企業資安評級之必要(1/2)

✓ 接軌國際發展趨勢：供應鏈資安成為標準配備



- ▲ 2020年美國國防部開始要求其供應鏈，需具備相應等級之「網路安全成熟度模型認證」(Cybersecurity Maturity Model Certification, CMMC)。
- ▲ CMMC2.0制定目的主要是**簡化與明確1.0的規範**，並帶動美國國防部與其承包商**資安聯防**，以因應日益複雜的網路安全攻擊。



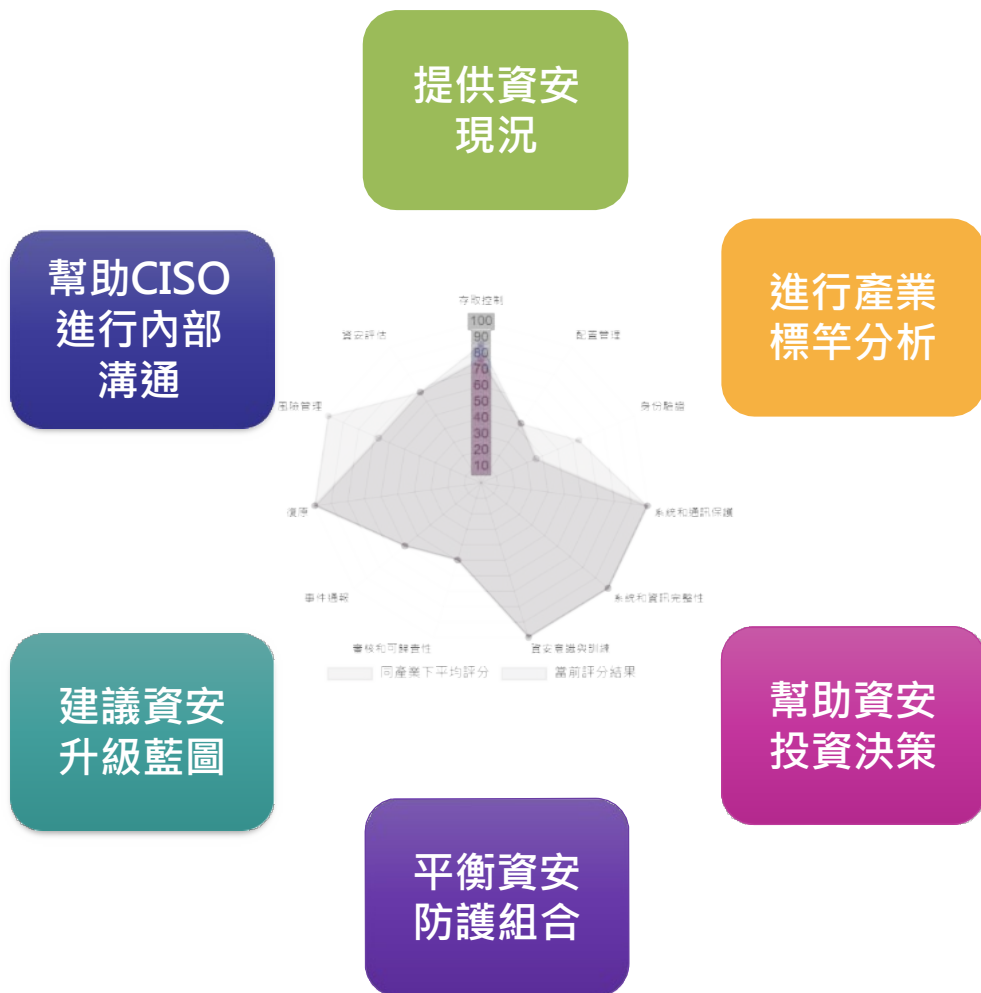
- ▲ 聯合國歐洲經濟委員會(UNECE)的世界車輛法規協調論壇(WP29)在2020年6月24日通過**兩個ECE法規要求：R155及R156**，且已於2021年1月份正式生效，到**2022年7月**，歐洲所有的新車型都需要遵守，到2024年7月，歐洲所有的車型都需要遵守。



- ▲ 由臺灣主導的半導體產業國際資安標準**E187**，已於**2022年1月正式公告**。未來半導體產業供應商、設備商將**依循此標準部署資安方案**。
- ▲ 本(111)年度將與SEMI合作共同推廣E187，包括教育訓練工作坊、標準導入實務測試等，協助臺灣相關產業導入E187，提高資安防護能力。

推動企業資安評級之必要(2/2)






✓ 執行資安成熟度評估好處



- ▲ 運用資安成熟度工具管理資安風險：
 - 讓資安的投資能夠進行**可視化**、**可量測**，以利於企業標竿管理
 - 改變過去只重視防火牆、防毒軟體的防護迷思，**平衡資安發展**
- ▲ 企業資安評級工具與服務：
 - 參照國際資安最佳實務，建立產業生態系的基本防衛能量
 - 對照**資通安全管理法**，協助產業進行內部**合規管理**
 - 掌握自身現況，**並透過持續性改善方法**，最佳化資安投資
- ▲ 產業需要重視資安委外的風險管理，企業資安評級可協助擴散至供應鏈廠商，以便於**掌握第三方資安風險**

企業資安評級-資安評級分類說明

- 參考NIST架構，以識別、防禦、偵測、回應、復原五大能力皆達成國際知名資安標準，將企業資安成熟度分成A、B、C、D、E五個等級

成熟度	資安評級定義	量化描述
	識別、防禦、偵測、回應、復原五大能力 已有良好能力確保 客戶或供應商的資通安全，除了有 標準作業流程 之外，並已完成 詳細資安防護計畫 。	資安健康狀況優良 估計已達成企業資安評級框架基礎版Level 1- Level 3(42項)的91%-100%資通安全要求。
	識別、防禦、偵測、回應、復原五大能力可以有 較佳的方法 保護客戶或供應商的資通安全，並且具有 標準化作業流程與記錄 ，並制定 資安相關公司規章	資安健康狀況尚佳 估計已達成企業資安評級框架基礎版Level 1- Level 3(42項)的76%-90%資通安全要求。
	識別、防禦、偵測、回應、復原五大能力 滿足基礎 資安防護能力，但可能還有 部分標準作業流程或公司規章尚未完善 ，但已具備 基本功 可以達到中階資安保護效果。	資安健康狀況適中 估計已達成企業資安評級框架基礎版Level 1- Level 3(42項)的41%-75%資通安全要求。
	識別、防禦、偵測、回應、復原五大能力 具備部分基礎 資安防護能力，可能 許多項目並無標準作業流程 ，但可以達到 基本保護效果 ，仍有改善空間。	資安健康狀況欠佳 估計已達成企業資安評級框架基礎版Level 1- Level 3(42項)的21%-40%資通安全要求。
	識別、防禦、偵測、回應、復原五大能力 尚未 能夠達到保護好客戶或供應商的資安基礎要求，也 缺乏標準作業流程與相關公司規範 。	資安健康狀況不良 估計已達成企業資安評級框架基礎版Level 1- Level 3(42項)的0%-20%資通安全要求。

企業資安評級顧問團輔導作業

單一企業之實地訪談輔導規劃

資安顧問輔導作業，預計2週完成：

1. 實地企業資安檢視網路架構圖、資安流程、人員、技術評估(一場訪視會議)
2. 資安顧問進行標準落差分析，協助進行改善優先排序
3. 提供客製化企業流程建置指引、資安建議部署方案(一場結案會議)

 前期
準備工作

1

1. 資安需求列表
2. 產生評估清單
3. 確定評估對象與時程



 展開
輔導工作

2

1. 現場/線上約談
2. 資料審核
3. 形成評估記錄
4. 評估具體情況



 完成
差距分析

3

1. 分析訪談記錄
2. 結合資安要求列表
3. 透果產業分析識別資安差距



 規劃
建構路線

4

1. 輸出訪談報告
2. 會報評估結果
3. 結合資安強化建議
4. 確定升級路線

線上
評估

人員
訪談

現場
查看

企業資安評級顧問協助方式

▲ 顧問資格

- 通過軟協資安能量登錄-資安顧問輔導、或SECPAAS上架資安服務業者
- 具有豐富資訊安全相關輔導實績的公司
- 顧問團隊熟悉NIST CSF、ISO27001或美國CMMC、IEC62443 2-1治理與資安管理概況
- 顧問團隊具有資訊安全相關認證資格人員，例如：ISO 27001主導稽核員;或行政院資安處認可之同等效力資安專業證照

▲ 執行內容

- 協助企業完成資安成熟度評估(產出初始評估報告)
- 完成企業資安現況檢視至少2場次(1場啟始會議、1場結案會議)
- 執行企業資安成熟度落差分析(優先排序、落後指標、領先指標說明)
- 提供資安不良實務說明與指引(改建建議、常犯錯誤舉例)
- 資安改善藍圖建議(含解決方案建議;不含方案採購評估)
- 完成1份資安成熟度結案報告(合規型)



**PART
05**

紅隊演練推動說明

紅隊演練 資安廠商申請資格

- **資安廠商的申請資格：**
 - 1) 為SECPAAS廠商
 - 2) 具備資安能量登錄的紅隊演練項目

演練目標	審查依據	提案組成	政府補助經費
<ol style="list-style-type: none"> 1. 驗證識別入侵途徑 2. 驗證資安解決方案的有效性 3. 協助企業藍隊解決重要弱點 4. 提高偵測弱點的效率資安防護與應變機制 5. 提升資安團隊的回應效率 6. 促進企業落實資安韌性提升 	<ol style="list-style-type: none"> 1. 確認企業資安防禦措施的有效性 2. 申請案件的總金額或預期金額 3. 驗證上市上櫃公司資通安全管控指引建議 4. 申請方期望解決的議題與企業營運方向及策略具備高度相關 	<p>資安廠商與一家「場域驗證企業」合作，採聯合提案</p> <p>*演練規劃 *合作意向書(MOU)</p>	<p>委員審核 每案補助 上限100萬</p> <p>由提案方主導規劃 提案經費，不足之處自籌</p>

申請資格-執行能力細項審核

徵案對象已建置防護項目	解決方案	資安法-A/B級機關資通系統防護基準	企業資安評級(CMMC v1.0)
資安團隊或IT兼資安人員	4-6人		
資訊安全管理制度(ISMS ISO27001)或個人資料管理制度(PIMS BS10012)	通過		
資安監控(SOC)委外/代建代維	一式	○	偵測、回應至少B級
APT流量側錄保存分析及Email檔案分析	一式	○	防護至少B級
資安健診	一次/半年	○	識別至少B級
弱點掃描	一次/半年	○	識別至少B級
滲透測試	一次/一年	○	識別至少B級
社交工程	一式	○	防護至少B級
在地/雲端網頁防火牆(WAF)、IPS服務、阻斷式攻擊防護(DDoS)	一式	○	防護至少B級
防火牆	一式	○	防護至少B級
防毒	一式	○	防護至少B級
郵件SPAM	一式	○	防護至少B級
加分項目: EDR/MDR 終端事件反應	一式	○	偵測、回應至少B級
加分項目:特權帳號稽核管理	一式	○	防護至少B級

申請文件審查標準

項目	內容	配分
計畫內容	<ul style="list-style-type: none"> • 產業背景與重要性 • 問題情境與需求痛點 • 資安技術導入目的與預期產生價值說明 	20%
執行能力	<ul style="list-style-type: none"> • 內部高階管理者參與 • 第三方技術單位或專家於資安經驗與專業度(如:演練場次、執行的產業類別) • 具有專利或技術驗證證明之國產資安合作廠商(MOU) 	35%
計畫效益	<ul style="list-style-type: none"> • 資安導入之效益與驗證方式 (審查紅隊演練實證規劃及紅隊演練複測效益) • 後續客戶或策略聯盟業者推廣計畫 (擴散效益) • 可帶動相關投資與營收、降低成本等經濟效益 (資安延伸效益) 	45%
加分項目	<ul style="list-style-type: none"> • 政府資安責任等級為B級或以上/企業資安成熟度B級或以上 • 專案金額 • IT或資安團隊的證照或相關經歷的履歷 • 與產業推動小組 (SIG) 合作，並簽訂合作意向書(MOU) 	5%

Q4資安Day成果發展：舉辦經驗分享會

- ◆ 目的：以經驗分享方式樹立示範，發揮帶動效果；協助企業驗證資安成熟度並補強資安缺口。

邀請對象1：資安廠商

內容：以企業/SIG產業脈絡-說明演練內容及資安缺口

- 1.藍隊優良品蹟
- 2.初測去識別化內容
- 3.複測的修補與強化

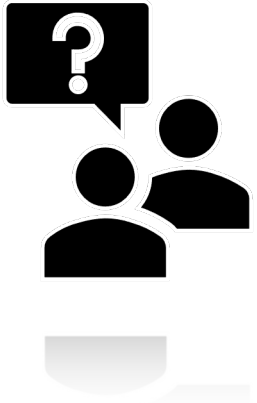
邀請對象2：公協會代表

內容：以企業/SIG產業脈絡-說明資安強化及升級效益

- 1.系統面- patch
- 2.非系統面- 佈署資安強化工具
- 3.產業產量/產值/供應鏈稽核分數/合規/訂單

- ◆ 基於機敏考量，保密及揭露資訊如下：

保密資訊	分享成果
<ol style="list-style-type: none"> 1. 受測公司基本資料 2. 資產資訊(如廠牌、規格、型號) 3. 漏洞利用細節 4. 限制性聽眾邀請 5. 特殊性資產 6. 能識別公司的數位資訊，包含：Public IP 7. 入侵的系統程式碼 	<ol style="list-style-type: none"> 1. 利用的CVE，可在CVE編號上末三碼去識別 2. 成功入侵的CVE，如：網站的2021-0930要注意 3. 產業類型 4. 通用性資產/" 類型" (如防火牆、端點防護、特權帳號等/資安防護：VDI系統/AD系統/email/醫院SHS) 5. 客戶已修正的入侵路徑可分享(點到為止) 6. 概括入侵路徑(入侵手法與入侵步驟) 7. 企業常犯的錯誤 8. 經驗反思及結語



Q & A



產業資安強化推動工作小組(SIG)

宋佳麟 專案經理

電話：04-2242-1717 #245

Email：lynn@tcca.org.tw

Thank you

