

跨境隱私規則(Cross-Border Privacy Rules, CBPR)簡介

財團法人資訊工業策進會

111 年 4 月

CBPR 是指跨境隱私規則，全稱為「Cross-Border Privacy Rules」。

CBPR 是在亞太經濟合作數位經濟指導小組（Asia-Pacific Economic Cooperation Digital Economy Steering Group, APEC DESG）下由美國領導推動的國際隱私法遵標準。

CBPR 透過參與的 APEC 會員經濟體共同建立國際隱私法遵一致性的要求，並藉由各國指定之當責機構（Accountability Agent, AA）對企業或組織進行驗證，證明企業或組織對資料或個資管理的重視與能力，建構合規資料自由流通的信賴環境，促進商務貿易往來。是 APEC 推動數位經濟發展基礎重要的一環。

APEC 在 2011 年正式實施 CBPR 之後，已有不少國家陸續獲得認可成為會員，至今除了臺灣之外，還有美國、墨西哥、加拿大、日本、韓國、新加坡、澳洲、菲律賓等會員經濟體，國際上亦有非 APEC 會員經濟體支持 CBPR，如百慕達等。未來也將持續有其他國家加入。

取得 CBPR 標章，採取透過第三方認證方式，證明企業資料保護具有相當水平，除了增加國際市場信賴度及商業機會，亦可有效減低個資法遵隱私風險。有助擴大數位貿易合作夥伴範圍，並於全球進行資料傳輸，銜接區域貿易資料流通。

更多說明如次：

1. CBPR 概述

- CBPR 是 APEC 下的跨境隱私規則，全稱為「Cross-Border Privacy Rules」。
- CBPR 是目前國際上唯一可與歐盟一般資料保護規則

(General Data Protection Regulation, GDPR) 相應的國際隱私法遵標準。

- APEC 遵循 CBPR 所建立的運作架構則稱為跨境隱私規則體系 (Cross-Border Privacy Rules System, CBPRs)。我國在美方促請下於 2018 年正式加入 CBPRs。

2. CBPR 如何運作？

- CBPR 是國際級驗證，且為我國政府參與 APEC 對於隱私保護之共同承諾。是 APEC 推動數位經濟發展基礎重要的一環。
- CBPR 透過參與的 APEC 會員體共同建立國際隱私法遵一致性的要求，並藉由各國指定之當責機構 (Accountability Agent, AA) 對企業或組織進行驗證。
- CBPR 可證明企業或組織對資料或個資管理的重視與能力，建構合規資料自由流通的信賴環境，促進商務貿易往來。

3. 除了美國、臺灣，還有哪些國家認可 CBPR？

- APEC 在 2011 年正式實施 CBPR 之後，已有不少國家陸續加入成為會員，至今除了我國之外，還有美國、墨西哥、加拿大、日本、韓國、新加坡、澳洲、菲律賓，共 9 個會員。全體 CBPR 成員貿易總額佔全球 39%。
- 我國則是在 2018 年加入 CBPR。成為會員後，國家發展委員會與隱私執法機關共同指定資策會，並由國家發展委員會指導及協助資策會申請作為 APEC 認證的 CBPR 當責機構。
- 2021 年 6 月 3 日終於獲得 APEC 認准，成為繼美國、日本、新加坡、南韓之後，第 5 個擁有當責機構的 APEC 會員體。
- 國際上亦有非 APEC 會員體支持 CBPR，如英國、百慕

達、杜拜國際金融中心等。未來也將持續有其他國家加入。

4. CBPR 是國際級驗證的意涵

- 所有通過 CBPR 驗證的企業可獲頒 CBPR 標章，彰顯遵循 APEC CBPR 一致性的隱私法遵要求，且受到 CBPR 參與國家的認可。

5. 如何取得 CBPR 標章？

- 向 AA 申請通過 CBPR 驗證之企業或組織，AA 得授權使用 CBPR 證明標章，彰顯企業或組織具備國際水準之隱私保護能力。
- 同時，通過 CBPR 驗證之企業或組織將登錄於 APEC CBPRs 官網通過企業或組織名單中。
- 詳參 CBPRs 官網：<http://cbprs.org/compliance-directory/cbpr-system/>

6. 什麼是當責機構(AA)？

- 當責機構的全稱是「Accountability Agent」，簡稱 AA。
- 目前全球有 5 個國家擁有 AA，共 9 個 AA，分屬於我國、美國、日本、韓國、新加坡等國。
- AA 可能是政府機關或法人組織，必須由所屬國家隱私執法機關（Privacy Enforcement Authority, PEA）推薦，向 CBPRs 聯合監督小組（Joint Oversight Panel, JOP）申請，經 APEC DESG 審查通過後取得資格。

7. 隱私執法機關與 AA 的關係？

- 按 CBPR 要求，國發會與我國 15 個隱私執法機關以經濟部 TPIPAS 寶貴的建置經驗為由，共同指定及推薦資策會擔任我國 AA。

8. AA 的任務是什麼？

- AA 主要任務是完成企業驗證（Certification）的執行，推動 APEC CBPR 此一標準的落實。
- 資策會科法所未來也將積極參與國際隱私活動，關注及研究國際隱私法制動向與最新發展，以利我國行政機關與私人企業之準備。

9. 全球有哪些企業取得 CBPR 驗證？

- 如 Apple Inc.、GE、EA、Cisco、IBM、MasterCard、Virgin Pulse、World Wrestling Entertainment、Alibaba Cloud (Singapore)、Paidy (Japan) 等。
- 詳參 CBPRs 官網：<http://cbprs.org/compliance-directory/cbpr-system>

10. 取得 CBPR 標章的優點

- 透過驗證流程，協助企業檢視其個資蒐集、處理、利用作業，結合流程診斷與優化，展現組織個資隱私保護優勢。
- 企業展現與國際知名企業同等級之個資管理能力，如 Apple、Cisco、GE、HP、IBM、Mastercard 等知名企業皆有通過 CBPR 驗證。
- 企業落實國際隱私法遵標準，跨境傳輸資料有保障。
- 增進與全球 CBPR 標章企業之互信與貿易機會。
- CBPR 標章組織 CISCO 於 2021 年調查，90% 的企業認為選擇供應商或產品時，是否取得隱私驗證為重要的考量因素。
- 增進消費者信賴與保障，消費者隱私意識抬頭，美國當責機構 TrustArc 於 2016 調查，美國消費者有 92% 對於網路隱私有顧慮。

CBPR機制說明

財團法人資訊工業策進會

科技法律研究所

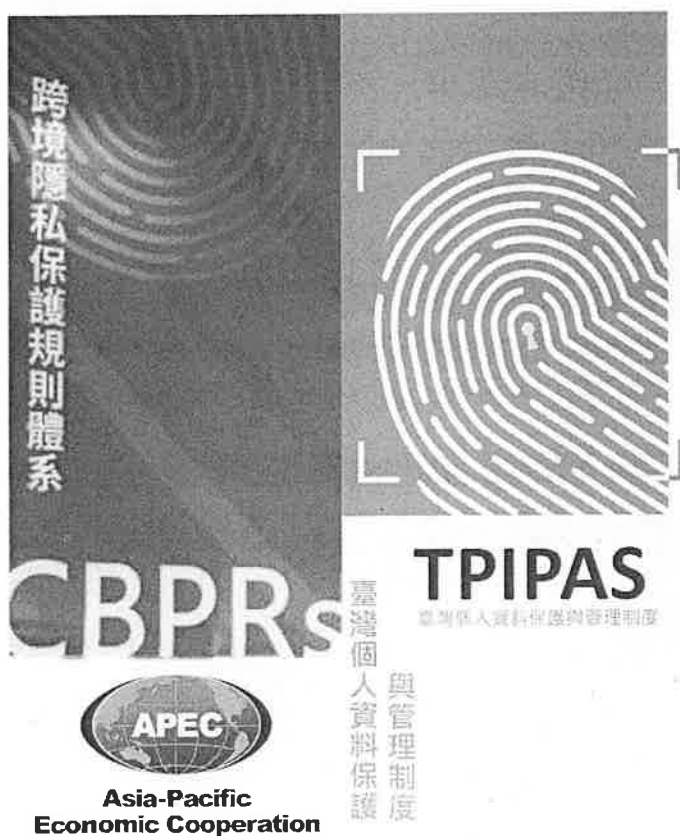
2022



tpipas@iii.org.tw
www.iii.org.tw

資訊工業策進會 Institute for Information Industry

資策會取得APEC隱私當責機構資格



資策會成為 APEC隱私當責機構！！



與APEC會員體隱私法遵接軌

- APEC CBPR為會員體互相認可的個資法遵驗證機制
- 資策會成臺灣首家APEC CBPR當責機構



彰顯企業個資隱私保護商譽

- 當責機構 (Accountability Agent, 簡稱AA) 負責驗證組織是否符合APEC隱私保護框架
- 搭配TPIPAS一驗雙證省成本·輕鬆接軌國際個資隱私保護標準
- 獲認證的組織更易於全球進行資料傳輸·推動區域貿易成長





簡報大綱

01

個資保護新觀念？
國際隱私新趨勢！

02

證明隱私保護力？
讓CBPR協助您！

03

如何取得CBPR？
事前準備工作須知！



01

個資保護新觀念？
國際隱私新趨勢！





全球個人資料保護的重要性

個資風險為科技風險之首

個資風險No.1



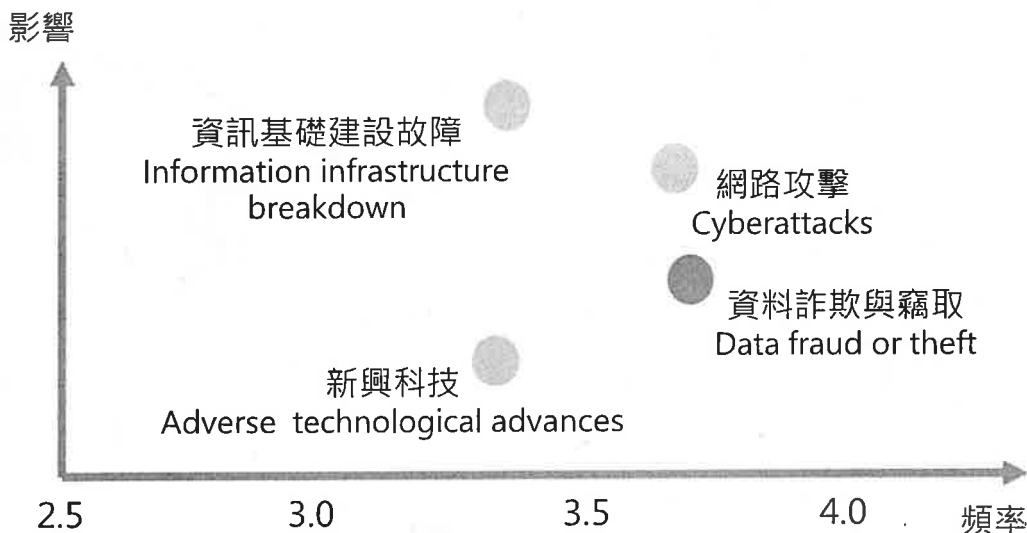
個資風險 > 資安風險



個人資料成為攻擊目標



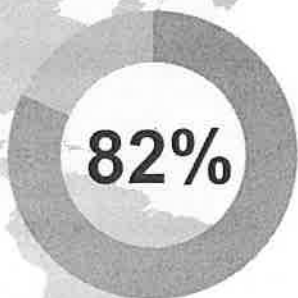
依據世界經濟論壇「2020年全球風險報告」指出，在科技風險類別中，「資料欺詐或盜竊」發生頻率最高，顯示機敏資料包含個人資料等成為攻擊目標的趨勢。



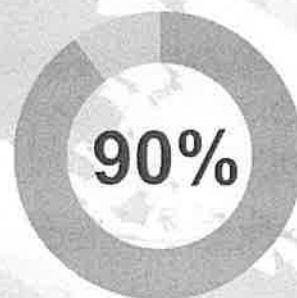
投資隱私保護的價值

隱私標章商業價值

2019年



2020年



90%企業將是否取得**第三方隱私認證**
 (如APEC CBPR、ISO27701或EU/Swiss-US Privacy Shield等)
 作為其選擇產品或供應商重要關鍵

資料來源：

CISCO 2020年「從隱私到利益：實現投資隱私的正報酬」報告、CISCO 2021年「資料隱私基準研究」報告



個資隱私保護生態圈建置邁向成熟



stli

6

2022 © 資訊工業策進會 Institute for Information Industry

PIMS 個資保護管理制度的重要性

PIMS 個資保護管理系統

ISMS 資訊安全管理系統

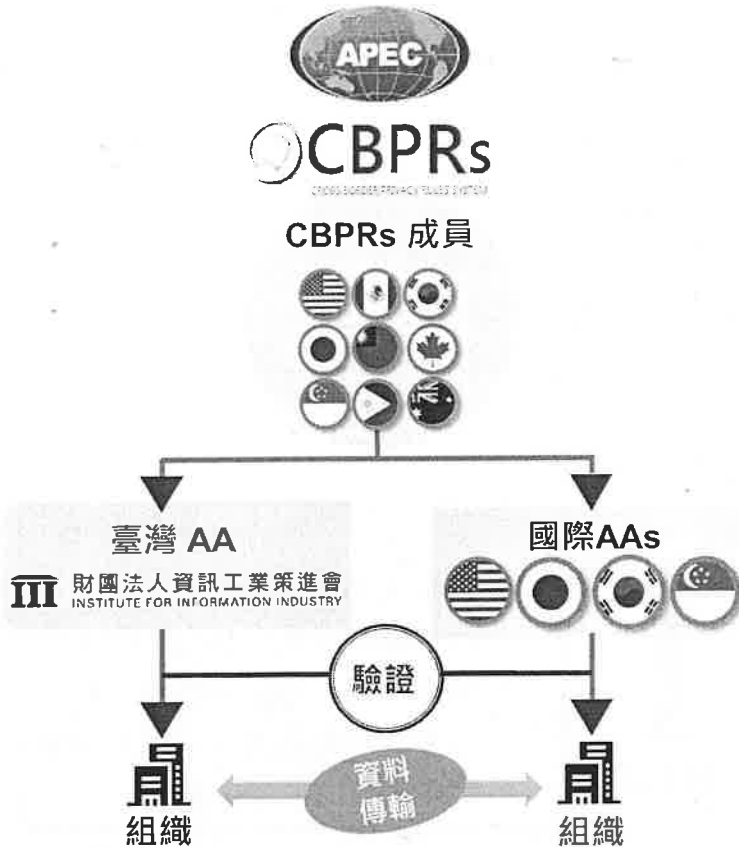


ISMS 著重於技術及細節面，PIMS 更強調組織文化及風險管理方法論。舉例而言，即使企業資訊化及數位化程度較低，於日常業務仍可能涉及員工或客戶個資保護處理議題。

7

2022 © 資訊工業策進會 Institute for Information Industry

🏠 跨境隱私規則體系 (CBPRs) 介紹



唯一亞太地區認可之驗證標準

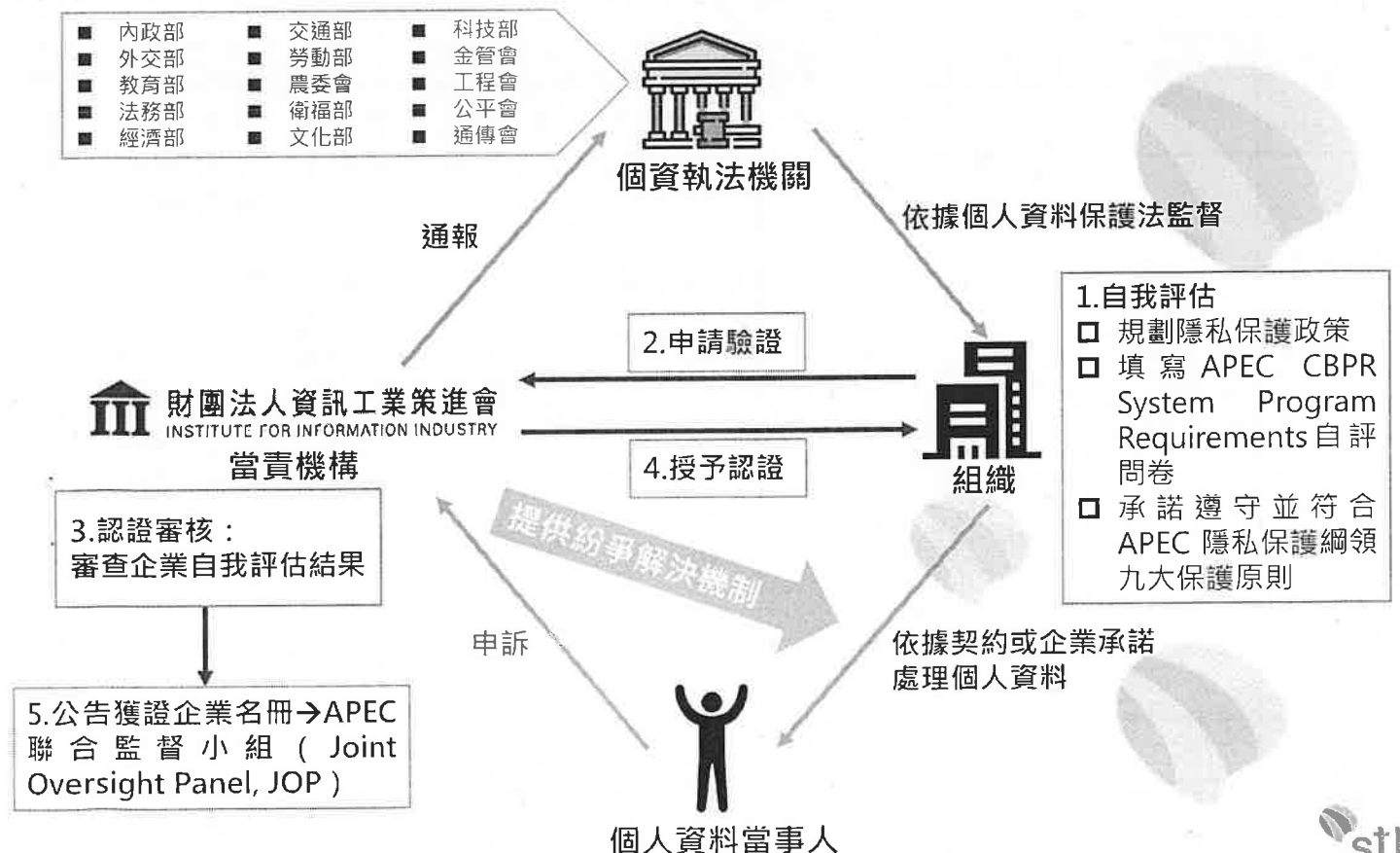
- CBPR為亞太地區唯一認可之國際級驗證，更是我國政府參與推動數位經濟發展基礎重要一環。
- CBPR透過參與APEC的會員體共同建立國際隱私法遵一致性的要求，並藉由各國指定之當責機構 (Accountability Agent, AA) 對企業進行驗證。
- CBPR可證明企業或組織對資料或個資管理的重視與能力，建構合規資料自由流通的信賴環境，促進商務貿易往來。
- 透過TPIPAS及CBPR驗證，檢視企業資料蒐集流程以改善內部資料治理與創新增加企業組織國際競爭力。



註：CBPRs 譯為跨境隱私規則體系；CBPR 為 CBPRs 認證標準，譯為跨境隱私規則



CBPR體系運作方式





CBPR與TPIPAS

● TPIPAS 臺灣個人資料保護與管理制度

- ◆ 經濟部自2010年推動之企業個資保護制度驗證

● APEC CBPRs 亞太經濟合作跨境隱私規則體系

- ◆ 我國CBPR驗證以TPIPAS為基礎，銜接CBPR之50道要求

- 鼓勵企業逐步完成個資管理制度建置，提高CBPR通過率
- 為鼓勵企業合併驗證，經國發會指導，一驗雙證可減輕企業時間成本外，可合併計算人天數，降低成本



- ✓ 一驗雙證：dp.mark+CBPR
- ✓ 落實法令遵循與資安防護
- ✓ 符合國家標準CNS29100-1
- ✓ 通過驗證，增加消費者信賴
- ✓ 符合合作廠商個資與資安要求
- ✓ 降低國際隱私法遵風險



CBPR+TPIPAS最符合國內外個資法要求

制度	CBPR	TPIPAS	BS 10012	ISO 27001	ISO 27701
性質	國際隱私法遵標準	個人資訊管理系統 (PIMS)	個人資訊管理系統 (PIMS)	資訊安全管理系統 (ISMS)	擴充 27001 增加對資訊安全管理要求
主導單位	APEC	我國經濟部	英國標準協會	國際標準組織	
特色	以國際要求銜接各國法遵規範，建立國際性一致性標準	<ul style="list-style-type: none"> ● 唯一依照我國個人資料保護法為基礎設計 ● 銜接 APEC CBPR 國際要求 	<ul style="list-style-type: none"> ● 僅適用英國境內 ● 主要依循 GDPR 設計 	第一個全球資訊安全管理的國際標準	包括： ISO27001 ISO27002 ISO29100
所涉法令標準	國際法	我國個資法	GDPR	國際標準	國際標準

向AA申請通過CBPR驗證之企業或組織，AA得授權使用CBPR證明標章，彰顯企業或組織具備國際水準之隱私保護能力。





02

證明隱私保護力？ 讓CBPR協助您！

stli

12

2022 © 資訊工業策進會 Institute for Information Industry



企業導入CBPR之效益說明

外國法令對跨境傳輸之限制

- 日本、新加坡已經將CBPR認列為跨境傳輸限制之例外情形；CBPR驗證目前落入美國聯邦貿易委員會管轄權
- 因應國際隱私保護趨勢，可透過CBPR提高我國重視跨境隱私保護之形象及創造跨國合作契機

- 協助我國參與和接軌國際資料傳輸制度挹注正面效果，獲得認證的組織更易於全球進行資料傳輸推動區域貿易成長
- AA任務包括審查與認證企業，並提供個資紛爭解決等機制，藉此強化我國企業建構個資保護制度

參與亞太經貿新秩序之形成

消費者端與供應鏈隱私要求

- 具有資料跨境傳輸並重視亞太地區市場之企業導入CBPR具有市場需求
- 證明企業資料保護具有相當水平增加國際市場信賴度及商業機會亦可有效減低因國際個資保護法制差異所產生之風險

- 個資法遵與資安標準不同，國際重視個資法遵對企業文化的要求與影響
- 取得國際認證標章將有助於展現資料管理實力，國際貿易交流進行跨境資料流通可節省企業操作時間與成本

企業並重個資法遵與資安標準

政府端

企業端

13

2022 © 資訊工業策進會 Institute for Information Industry

stli



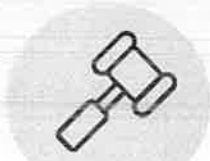
CBPR為數位時代隱私保護利器



財務面

建置與投報率正相關

隱私建置高度成熟的企業於各項指標表現佳



法令遵循面

日益嚴格的法規環境

隱私保護意識抬頭，

各國紛紛制定隱私保護相關法規



策略面

有助於進軍潛力市場

有助進入科技、醫療、金融等資料
高度機敏產業



CBPR



風險管理面

風險管理方法論

不僅強調組織企業文化，同時融入PDCA方法論



政策面

PIMS不等同ISMS

政府以政策鼓勵高風險行業取得PIMS認證



財務面：隱私保護的投資與回報率(1/2)

	2019年	2020年
年度平均隱私支出	120萬美元	240萬美元
隱私投資回報 (包含增加的選商競爭優勢、減少銷售延遲及降低訴訟成本等)	40%企業評估投資隱私至少帶來2倍的投資收益	雖然受疫情影響，隱私投報率略為降低，然而仍有35%企業評估投資隱私至少帶來2倍的投資收益
隱私保護驗證	82%的組織認為選擇供應商或產品時，是否取得隱私驗證（例如APEC CBPR、ISO27701 或 EU/Swiss-US Privacy Shield等）是選擇產品或供應商的重要因素	90%的組織認為選擇供應商或產品時，是否取得隱私驗證（例如APEC CBPR、ISO27701等）是選擇產品或供應商的重要因素

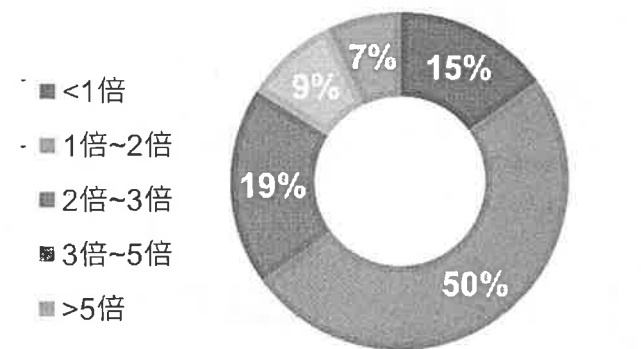
1. 93%組織向隱私團隊尋求疫情大流行的應對措施。
2. 79%組織認為隱私法具有正面影響。
3. 93%組織將隱私相關議題向董事會報告。

資策會站在推廣個資保護角度，並根據APEC建議，將驗證成本保持在市場最低水準，適度降低廠商進入的財務門檻及負擔。



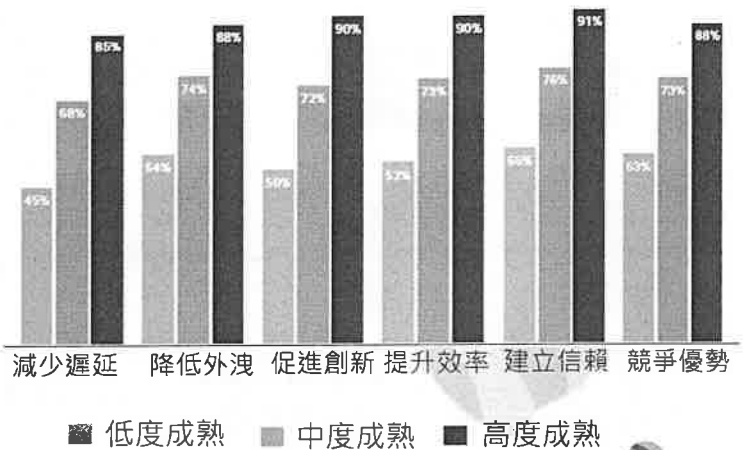
財務面：隱私保護的投資與回報率(2/2)

● 投資隱私成熟度與績效指標呈正相關



將近七成企業投資隱私的回報率約落在投資隱私成本之**1~3倍**

隱私保護制度**高度成熟**的企業在各項指標表現皆**最佳**



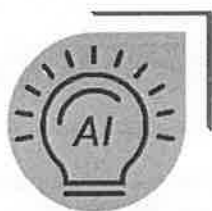
CISCO 2020年「從隱私到利益：實現投資隱私的正報酬」報告、CISCO 2021年「資料隱私基準研究」報告

16

2022 © 資訊工業策進會 Institute for Information Industry



策略面：取得隱私產業先機



人工智慧與科技產業

- 2021年歐盟執委會發布《人工智慧管理法》草案，強化透明性義務
- 依據風險程度，設有不同密度規範，以兼顧科技發展與人權價值



生技醫療與照護產業

- 健康醫療數據首重個資隱私保護，用戶願意分享其私密資訊，需要深厚的信任關係
- 隱私保護範圍涵蓋個人隱私及資訊安全需求



數位金融與保險產業

- 數位金融三大趨勢：大量運用API、跨平台動態串流資料存取；及開放資料加值運用
- 有效控管數位足跡強化客戶信心，兼顧大數據應用及隱私議題

將隱私作為產品開發設計的基礎建立用戶信任，有助於產業進軍高度敏感資料領域，為極具潛力與商機的市場

17

2022 © 資訊工業策進會 Institute for Information Industry

政策面：CBPR為國際頂尖企業的選擇



<http://cbprs.org/compliance-directory/cbpr-system/>



18

2022 © 資訊工業策進會 Institute for Information Industry

風險管理面：強化組織內控三防線

1 第一道LOD

Business Line
業務單位

**Owns the risk-
掌握風險及控制責任**

透過驗證程序，組織得：

- 確認個資隱私風險暴險額度控制在風險胃納中
- 辨認、評估、控制其業務所面臨
- 定期掌握組織內部風險變化及改善程度

2 第二道LOD

Corporate functions
風控小組、法遵等部門

**Governs the risk-
控制、整合、監督風險**

- 依據CBPR九大標準檢視並修正個資管理政策
- 藉由全域驗證整合不同部門風險
- 確保業務單位風險已經被適當的辨認及管理
- 評測風險並向公司管理階層彙報

3 第三道LOD

Independent audit
內部稽核

**Provide assurance-
提供獨立內稽評估**

- 透過每年外部驗證程序與內部稽核機制相輔相成
- 對組織內控制度有效性提供一定保證
- 透過定期驗證與主管階層彙報查核結果



19

2022 © 資訊工業策進會 Institute for Information Industry

法令遵循面：現行個資檔案安全維護規範

主管機關	業別	辦法數
經濟部	網際網路零售業及網際網路零售服務平台業、自來水事業、製造業及技術服務業、電業及公用天然氣事業、著作權集體管理團體	5
金管會	金融控股、銀行、保險、證券、期貨、電子支付、其他經金管會公告之金融服務業、金管會主管之財團法人	1
通傳會	第一、二類電信事業、有線廣播電視、電視、衛星廣播電視、經營國內新聞台或購物頻道事業等六類	1
交通部	停車場經營業、旅行業、民用航空運輸業、船舶運送業、觀光旅館業、觀光遊樂業	6
教育部	海外臺灣學校及大陸地區臺商學校、短期補習班、私立兒童課後照顧服務中心、私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、運動彩券業	6
內政部	保全業、槍砲彈藥刀械業、殯葬服務業、移民業務機構、當舖業、營建類非公務機關、地政類非公務機關、警政類非公務機關、合作及人民團體類非公務機關、祭祀團體、政黨及全國性民政財團法人、宗教團體	12
勞動部	人力仲介業、私立職業訓練機構	2
衛福部	精神復健機構、護理機構、醫院、西藥批發零售業、醫療器材批發零售業、非輻射電子醫療器材設備製造業、食品業、化粧品批發零售	8
財政部	公益彩券發行機構、菸酒事業、記帳士與記帳及報稅代理人、保稅倉庫物流中心	4
公平會	多層次傳銷業	1
工程會	工程技術顧問業	1
原能會	游離輻射設備製造業	1
中央銀行	票據交換所	1
農委會	農業金融、農藥販賣業	2
大陸委員會	大陸委員會指定非公務機關	1
合計		52

統計截至2022/01

20

2022 © 資訊工業策進會 Institute for Information Industry



03

如何取得CBPR? 事前準備工作須知!



CBPR 驗證機制介紹



若企業內部已具備個資管理制度？

	TPIPAS	其他PIMS/ISMS標準 (如 ISO27001、27701 ; BS10012)
可否加驗 CBPR ?	可以	可以
說明	<ul style="list-style-type: none"> 為鼓勵企業階段性完善個資管理制度，優先通過經濟部TPIPAS驗證後，再逐步升級國際級的CBPR驗證。 除提供減免優惠外，企業可透過一驗雙證方式合併計算驗證人天數，同時完成TPIPAS與CBPR之驗證，節省企業驗證之的行政及時間成本，輕鬆接軌國際隱私法遵標準。 	<ul style="list-style-type: none"> ISO27001、27701屬於資安為主之標準；BS10012為英國個人資訊管理系統標準，與我國制度仍存在差異，兩者均未完整符合國內法遵或CBPR要求。 因此，為確保符合CBPR要求，仍須經完整檢視，無法合併計算驗證人天數。

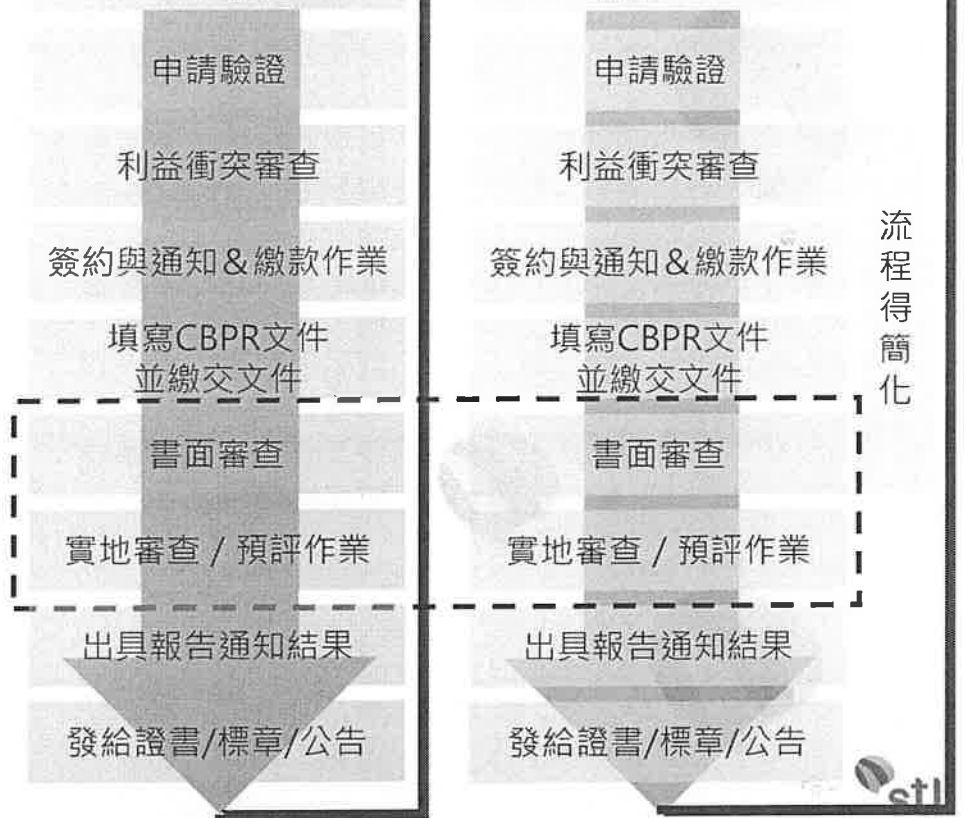


CBPR初次驗證及更新驗證

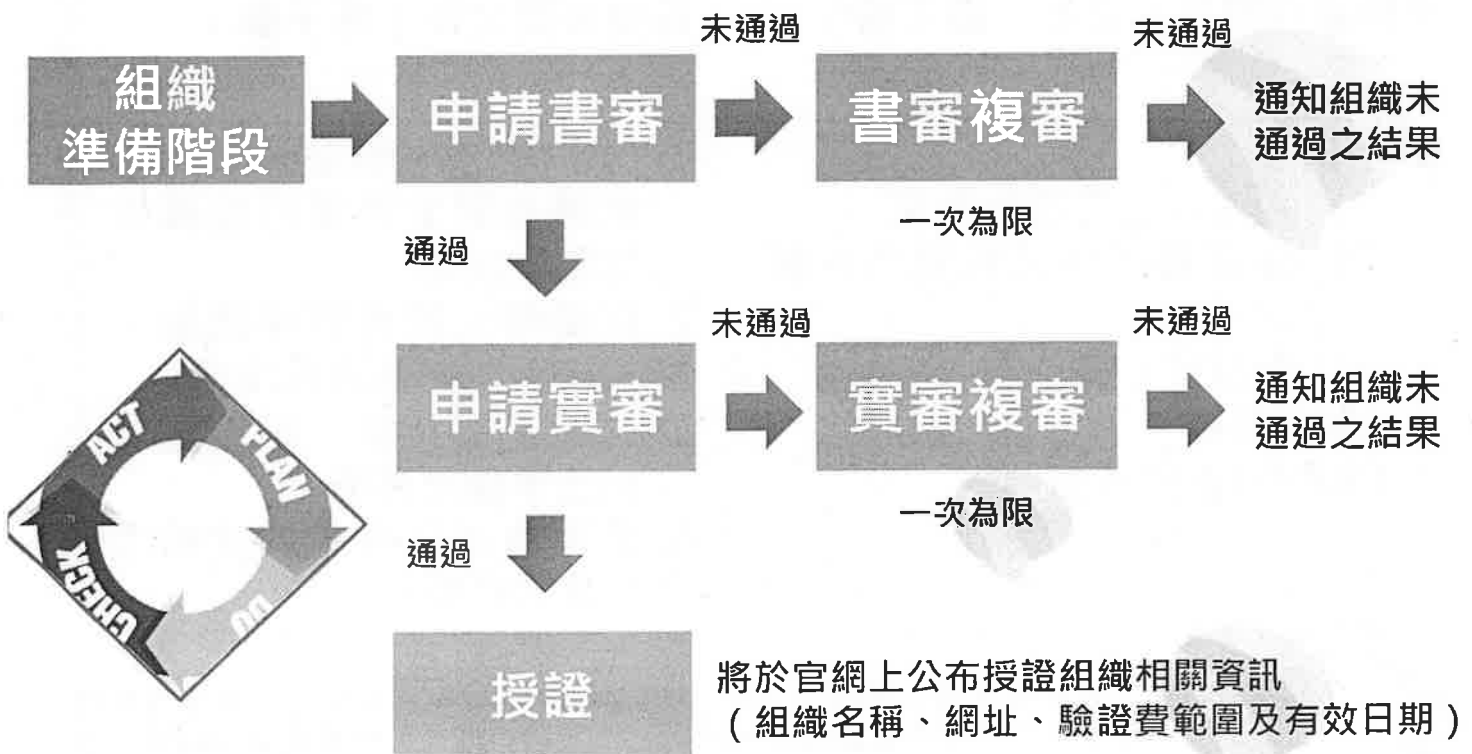
結合APEC CBPR System Program Requirements 與臺灣個人資料保護與管理制度規範 (TPIPAS)

初次驗證

更新驗證 (每年)



驗證流程概覽





驗證流程與準備項目

準備階段

1. 建議至少培訓TPIPAS管理師與內評師各2名。
2. 透過CBPR問卷，瞭解組織內部個資管理情形。
3. 依CBPR計畫備妥個人資料管理政策、管理手冊、各項程序書及相關制度文件，並予以落實執行。

申請階段

1. 填妥CBPR驗證申請書與附件（包含CBPR問卷與對照表）。
2. 檢附現行組織架構圖、個人資料管理政策、管理手冊與各項程序書等文件。
3. 向當責機構提出申請，並完納費用。

驗證階段

書審階段：

1. 當責機構於組織提交驗證申請書與相關文件後進行書審階段。
2. 書審階段後，組織應依通知完納實審費用，並與當責機構確定實審驗證日期。

實審階段：

1. 當責機構於驗證日期當天至組織實地實審。
2. 通過實審後，組織應依當責機構通知完成後續授證程序。



所需準備文件

申請書與附件（紙本、電子檔）

1. 申請書
 - 1) 組織利益衝突聲明單
 - 2) 個資管理師及個資內評師資料表
 - 3) 內評資料表
2. CBPR問卷
3. CBPR計畫要求對照表

其他必要文件（電子檔）

1. CBPR計畫要求對照表內容所涉相關文件現行組織架構圖及說明
2. 組織個人資料管理政策、管理手冊與各項程序書
3. 個資流程文件、個資清冊與法令盤點清冊
4. 最近六個月內完成之組織年度內評報告



資策會將站在推廣個資保護角度，並根據APEC建議，將驗證成本保持在市場最低水準，適度降低廠商進入的財務門檻及負擔。更多費用項目說明，敬請聯繫當責機構資策會科法所。



如有任何疑問

歡迎與我們聯繫



Phone

專線服務：(02) 6631-1069



Email

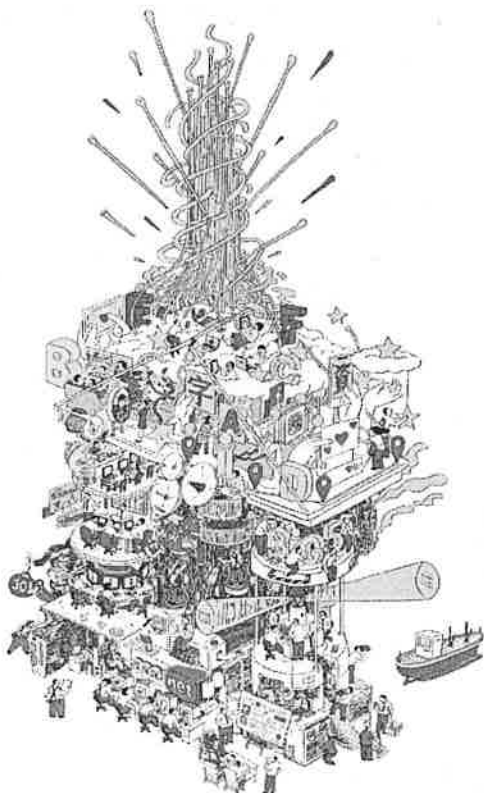
TIIPAS信箱：tpipas@iii.org.tw



TIIPAS官網



<https://www.tpipas.org.tw/>



- 1.鞏固我國資訊工業發展藍圖
- 2.開啟電腦中文文化時代
- 3.打造台灣資訊品牌
- 4.培養台灣資訊人才
- 5.開創產業顧問服務
- 6.提升網路基礎建設
- 7.化政府系統
- 8.普及網路應用人口
- 9.建構資訊法案制度
- 10.縮減城鄉數位落差
- 11.推動數位內容
- 12.推動數位科技外交
- 13.策進 e-Taiwan / m-Taiwan
- 14.精進5G智慧科技創新應用
- 15.支援文創與設計產業奠基
- 16.培育創新創業新動能
- 17.擔任數位國家智庫
- 18.活化原鄉無線寬頻環境
- 19.協助產業拓展商機並強化資安防護
- 20.數位轉型化商者

THANK YOU



