TAIWAN STOCK EXCHANGE
臺灣證券交易所

資通安全查核重點及缺失案例分享

券商輔導部

TAIWAN STOCK EXCHANGE
臺灣證券交易所

大綱

- 資安查核重點
- 監理科技運用
- 資安通報案例

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

證券商電腦稽核之法源

臺灣證券交易所股份有限公司查核證券商作業辦法

- 第1~11條說明辦理查核依據及方式

建立證券商資通安全檢查機制

•91.2.21台證（九一）稽字第003551號，修訂「建立證券商資通安全檢查機制」檢查項目，並自91.4.1日起實施。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

年度資安例查

- 檢視證券商整體資安防護 及 法規落實情形

選案查核

- 投資人檢舉、主管機關指示、主機共置服務

專案查核

- 特定議題對市場之影響 或 檢視整體辦理情形

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

資通安全檢查機制

- 辨識資安風險
- 訂定資安政策
- 配置組織資源
- 清查資訊資產
- 強化人員管理
- 監控環境設備
- 管理通訊作業
- 落實存取控制
- 控管開發維運
- 提升營運韌性
- 實作規範相符
- 納管新興科技

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

風險評鑑管理

1. 評估可接受之資安風險等級
2. 風險評鑑報告、風險改善計畫(每年產出)

資訊安全政策

1. 定期評估資安政策
2. 發布員工、廠商知悉
3. 建立「資安、個資通報程序」

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

安全組織

1. 評估資安人力配置
2. 取得資安專業證照
3. 資安長設置 (13家)

資產分類與控制

1. 編列資訊資產清冊
2. 每年評估資訊系統妥適分級
   (核心、非核心)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

人員安全

1. 完成資安教育訓練(含物聯網)
2. 取得訓練時數證明

實體與環境安全

1. 制定「資訊設備報廢」規範、留存報廢紀錄
2. 制定「機房門禁管制」規範、定期審查權限

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

網路安全管理

1. 依用途區分網路
   (DMZ區、營運環境、測試環境、其它環境)
2. 適當區隔機制(防火牆、區域網路、實體隔離)
3. 核心系統應建置於防火牆內
4. 不使用危害國家資通安全產品

網路安全管理

5. 遠端連線應使用安全連線機制、登入應採多因子驗證
6. 適時修補網路設備、作業系統之安全漏洞
7. 評估已停止支援服務(EOS)設備的汰換、升級計畫
8. 評估防火牆管控規則、進出紀錄保存3年

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

網路安全管理

9. 伺服器及個人電腦應安裝防毒軟體、更新病毒碼、定期掃描

10. 偵測系統內「網頁及程式」異動紀錄、通知相關人員

11. 制定「電子郵件安全」規範、設定安全性規則(以純文字檢視、關閉自動下載圖片)、過濾惡意軟體

網路安全管理

12. 建置「入侵偵測 (IPS) 防禦機制」、
建置「網站應用程式防火牆 (WAF)」

13. 制定「網路下單服務品質標準」，包含「交易安全性、穩定性、系統可用性、提供給客戶的服務」；
並對可用性進行評估(壓力測試報告)

資安查核重點

網路安全管理

14. 防範撞庫攻擊：每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄進行監控及分析
15. 對於嘗試登入帳號之異常及不明來源IP，建立警示機制，進行監控分析及留存紀錄
16. 建立通知客戶機制(簡訊、APP 或 Email)，確認是否為客戶本人登入

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

電腦系統及作業安全管理

1. 制定「軟體安裝作業程序」
2. 建立軟體白名單、黑名單

存取控制

1. 制定「最高權限帳號管理辦法」，管控使用，留存紀錄
2. 定期盤點帳號使用情形、檢討久未使用之帳號
3. 人員異動應即時更新帳號權限、不可共用帳號
4. 設定密碼複雜度、密碼長度、使用期限 (文數字、符號、6碼以上、90天)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

存取控制

5. 核心系統稽核日誌(log)應紀錄使用者識別碼、登入日期時間(供日後稽核使用、鑑識)
6. 管控機敏資料，防止外洩；妥善管理 測試環境中的 正式資料 (依規定申請、適當遮蔽個資)
7. 網路登入、下單應採多因子驗證

存取控制

8. 線上交付憑證應採多因子驗證，且需與登入時使用之因子不同
9. 定期盤點帳號使用情形、檢討久未使用之帳號
10. 盤點個資、留存操作軌跡、加密傳輸機制
11. 電子式專屬線路下單（DMA）使用合規，交易及稽核紀錄保存五年

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

系統開發及維護

1. 委外合約應包含「資訊安全協定」及「委外稽核權」
2. 資訊服務供應商之選定過程，應留下風險評估紀錄(如財務狀況、專業能力)
3. 程式變更之管控程序，應包含日常及緊急作業
4. 每半年辦理一次資訊系統「弱點掃瞄作業」

系統開發及維護

5. 評估系統已知弱點之修補方式，留存紀錄；修補完成後再次掃描
6. 每年將APP交付合格檢測實驗室，並通過資安驗證，針對報告進行覆核
7. 訂定API服務規範，投資人首次使用API委託下單前，應進行連線測試

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

系統開發及維護

8. APP如涉及「下單交易」、「帳務查詢」、「身份辨識」之功能異動，上架前應再次自行或委外通過檢測
9. 委外開發之APP應檢視資料傳送對象之適當性，並留存相關紀錄
10. 核心系統上架及更新時，應執行源碼掃描安全檢測
11. 使用第三方服務時，應制定相關規範進行管控

持續營運管理

1. 建立DDoS防護機制
2. 主備線路導入流量清洗機制
3. 訂定核心系統可容忍中斷服務時間
4. 訂定持續營運應變計畫
5. 備援程序演練、故障復原程序演練
6. 建立資料保存及備份機制，防範勒索病毒

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

符合性

1. 每年辦理資訊安全查核作業1次
   （內部辦理 或 委託外部專業機構）
2. 針對資安查核報告，確實辦理追蹤改善

新興科技應用

1. 使用雲端服務時，應制定「雲端運算服務運作安全規範」
2. 訂定「社群媒體管理辦法」(內容過濾與監視)
3. 訂定「員工使用自攜行動裝置管理規範」
4. 訂定「物聯網安全規範或管理辦法」
5. 每年更新「物聯網設備管理清冊」

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

前三級證券商適用

1. 核心系統導入國際資安標準 (ISO 27001)
2. 建立「防範網路釣魚機制」
3. 辦理滲透測試，評估修補作業流程
4. 辦理資安健診，包含「網路架構、網路惡意活動、伺服器主機、防火牆設定檢視」

(一級 證券商 「每年」 辦理1次
二三級 證券商 「每兩年」 辦理1次)

前三級證券商適用

5. 妥善處理線上開戶之客戶資料
(婉拒開戶、未前往開戶，應有資料刪除機制)
6. 建立資通安全威脅偵測管理機制
(建置資安監控中心)
7. 核心系統辦理原始碼檢測作業
(包含掃描週期、掃描工具及後續修補情形)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核重點

一二級證券商適用

1. 建立「進階持續性威脅(APT)」防禦系統(可自行或委外)
2. 依據F-ISAC情資，進行資安強化作業
3. 定期辦理社交工程演練，並針對未通過之人員進行資安教育訓練

TAIWAN STOCK EXCHANGE
臺灣證券交易所

監理科技運用

導入大數據分析工具

「資安風險現況」 儀表板

- 以風險為導向，依據證券商「電子交易比重」及「查核缺失扣分」，定義風險區塊，找出需要關懷的證券商，加強輔導，協助改善。

「風險趨勢分析」 儀表版

- 分析證券商家數占比最高的「缺失類型」及「增減趨勢」，關注重要資安議題，找出「隱藏風險」，精準輔導，提升防護能力。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安通報案例

資安通報案例

通報案例1：委外廠商系統異常 (1日內發生2起同類型)

1.APP電子下單主機異常，無法登入

- 經查下單主機相關設定均無異常，最後將主機中內建的「Windows Defender防火牆」關閉後，連線即恢復正常。

2. APP電子下單系統，連線異常

- 因中台主機作業系統更新後，內建的防毒軟體導致連線異常，後續將作業系統回復舊版，連線即恢復正常。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安通報案例

分析原因

- 應是微軟在當日發布系統更新，維護廠商安裝更新檔後，系統上原本已開通之連線服務，被更新後的預設值給覆蓋掉（預設值為「封鎖」），導致連線異常、服務中斷，影響客戶下單交易。

對應作為

- 應謹慎評估作業系統升級或程式更新後的影響，並經過完整測試後再進行升級，同時應有效掌握維護廠商所提供之服務內容。

通報案例2：委外廠商系統異常

憑證系統驗章回應緩慢，造成電子交易平台無法登入

- 經查資料庫資源使用正常，係因憑證系統應用程式無法提供連線服務，將憑證系統主機重開機、重啟服務之後，連線即恢復正常。

通報案例2：委外廠商系統異常

分析原因

- 憑證伺服器與資料庫連線之程式存在設計瑕疵，當使用者完成憑證驗章後無法順利結束連線並釋出連線資源，造成系統資源被持續占用，當達到系統承載上限後，即無法再提供資源給下一位使用者，造成憑證驗章服務中斷。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安通報案例

應變方式

營運持續計畫

業務持續運作演練(BCP)

執行	切換
故障復原程序	備援系統

RTO 復原時間目標

客戶服務不中斷

1.第一時間公告	1.妥善處理客訴
2.引導投資人採用替代方式下單	2.統計受影響人數 預估受影響金額

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安通報案例

後續處理

依規定通報

資通安全通報系統	MIS公告
30分鐘 初步通報 24小時 正式通報 3 天內 解除通報	即時公告 (涉及 影響交易、影響投資人權益)

系統開發及維護

程式開發	壓力測試
1.掌握核心架構 2.Code review 3.優化程式效能	1.擴大壓力測試 2.系統資源分配 (應用程式主機、資料庫主機、憑證主機)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安通報案例

諮詢服務

證券業者資安應變與諮詢服務	
資安事件 電話關懷服務 協助於30分鐘內完成初步通報	全天候(7X24小時) 應變處理電話諮詢 協助於24小時內轉為正式通報

TAIWAN STOCK EXCHANGE
臺灣證券交易所

簡報結束
敬請指導

Deloitte.

勤業眾信

國際資安認證 - 強化資安競爭力

勤業眾信 | 風險諮詢服務部門 | 2023.07

Agenda

- 網路安全發展趨勢
- 國際標準管理制度控管精神分享
- 國際標準管理制度導入效益
- 意見交流

網路安全發展趨勢

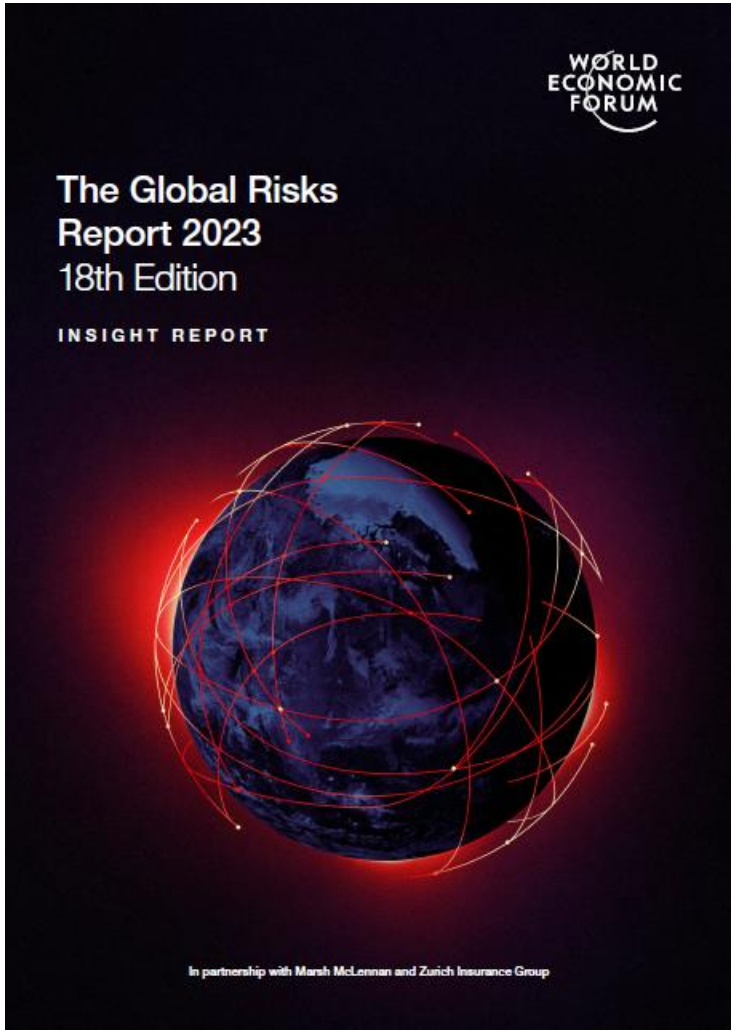
全球風險趨勢

全球經濟論壇(WEF)警示因各國科技發展不平等加劇，而網路安全風險仍將是一個須密切關注的議題

科技發展一向都是各國家核心目標之一，新興科技的研發將在未來十年繼續快速發展，並著重在**人工智能、量子計算和生物技術**等技術領域。

然而，新興科技的快速發展和部署往往伴隨著有限的規範管理。由其對於無法跟進科技發展之國家，從**散播大量錯誤虛假資訊等網路攻擊**至藍領和白領工作快速流失，**不平等和分歧將會加劇。**

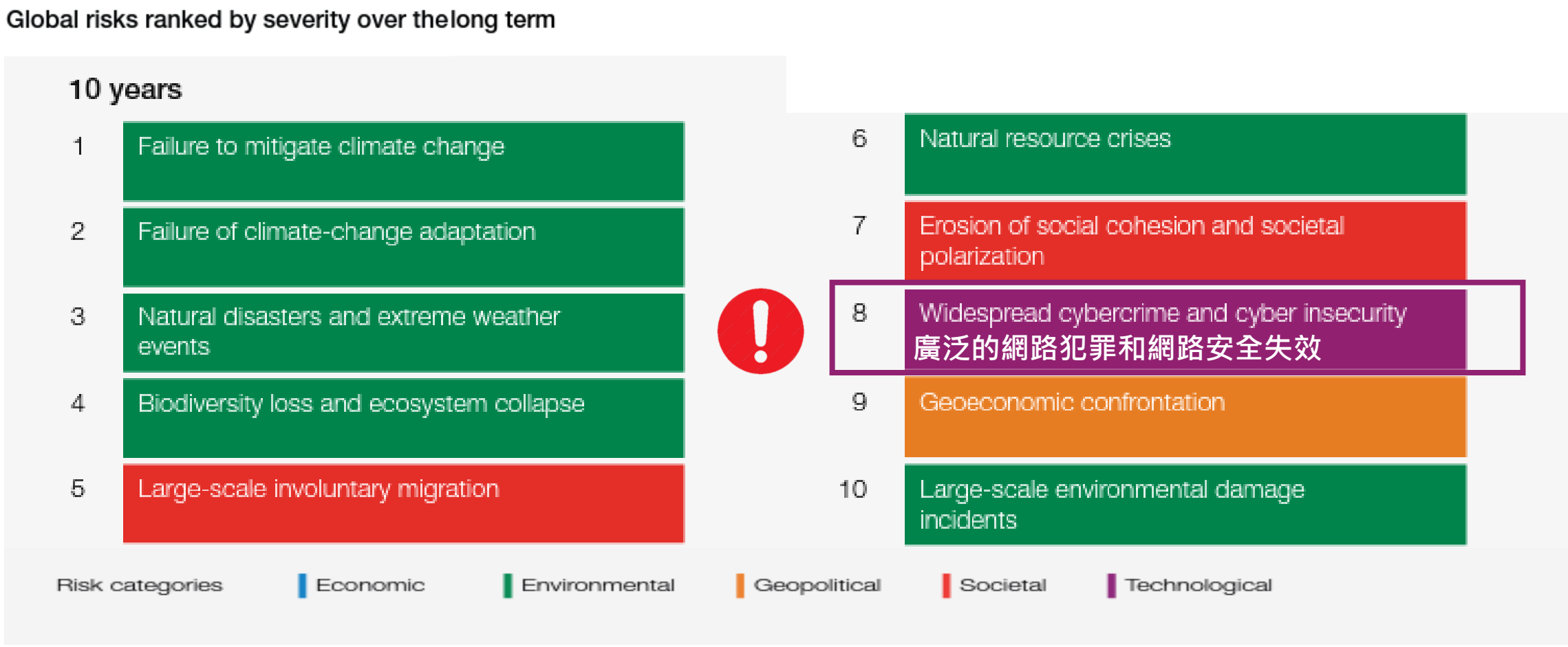
針對國家**關鍵基礎設施的網絡攻擊**已被列為2023 年全球性風險前五名。



Source: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

「廣泛的網路犯罪和網路安全失效」是未來十年風險排名前10名的新成員。

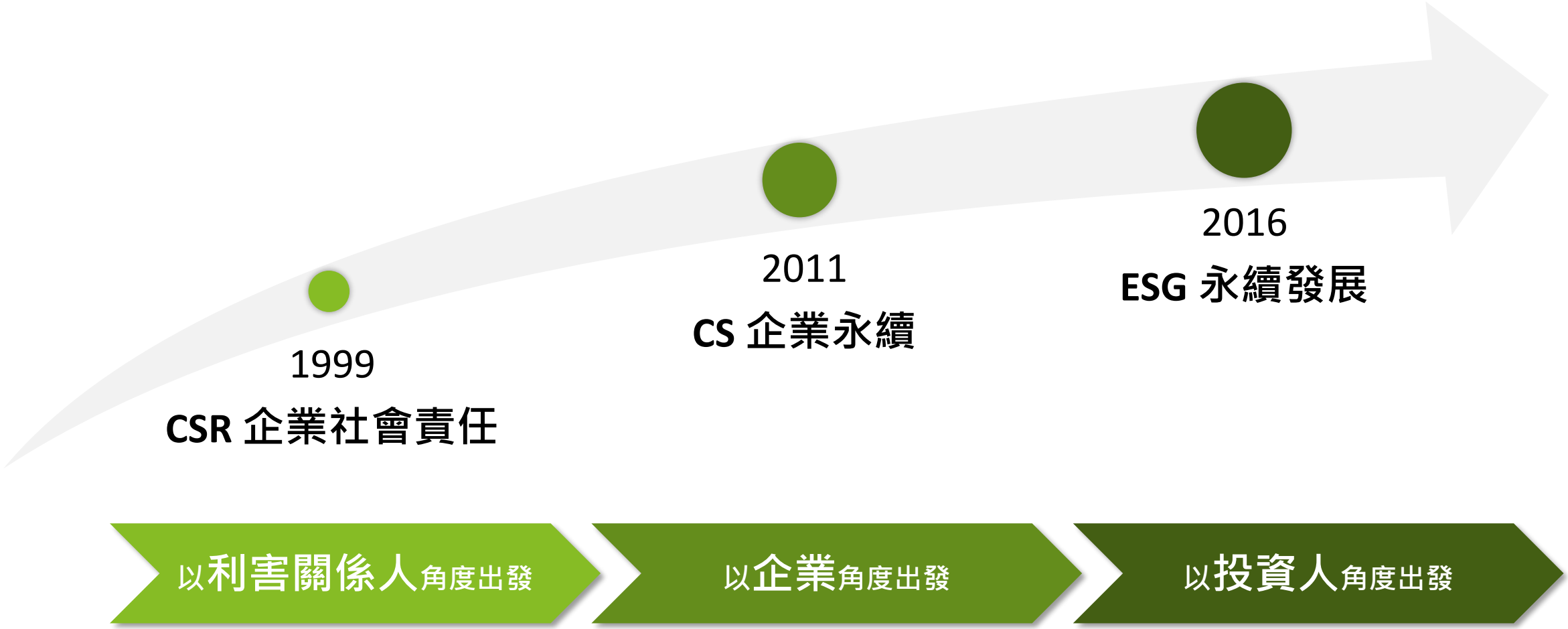
根據世界經濟論壇2023年報告指出，「廣泛的網路犯罪和網路安全失效」是未來十年風險排名前10名的新成員。



Source: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

企業永續發展：從 CSR 到 ESG

近年來興起「**責任投資**」風氣，國際投資人或評比機構重視企業「永續發展（即公司治理、社會、環境，ESG）」管理，從「ESG風險管理」角度出發，評估企業長期獲利績效



ESG概念影響廣泛

ESG一反過往僅關注財務表現，而將環境、社會和公司治理等因素納入企業經營之考量，ESG管理成熟度會為公司經營穩定度和聲譽帶來一定影響，也會影響投資人的對企業的投資決策

- 氣候風險
- 天然資源稀缺
- 能源使用管理
- 汙染及廢棄物管理
- 生物多樣性

- 員工健康管理
- 勞資關係
- 資安隱私權維護
- 產品責任
- 客戶福利

- 商業倫理
- 董事會素質與成效
- 供應鏈管理
- 風險評估管理

ESG成為上市櫃公司競爭追逐的目標，進一步推動企業邁向數位轉型之路

將 ESG 嵌入數位轉型的核心競爭力，識別和執行具有競爭力的營運策略。

ESG 策略目標與考量

- 經濟績效、採購實務與反貪腐
- 碳排放、碳足跡、供應鏈環境評估
- 原物料、水資源、汙水與廢氣物處置
- 員工多元與公平機會、職業安全、勞雇關係
- 產業願景與國際政策、企業形象
- 社會經濟法規遵循、客戶安全與隱私

規劃數位轉型藍圖

關鍵推動項目

- 建立跨境溯源機制
- 供應鏈碳排放與碳足跡檢查與追蹤
- 科技賦能與創新

各方期待

市場、客戶、投資者、產業

董事會、CXO 訂定

- 集團願景
- 策略目標

擬定策略

- QCDS管理
- 評估上下游衝擊
- 控管ESG風險
- 接軌國際間企業碳排管理趨勢

ESG x 數位轉型策略

- ESG 願景、指標、與治理
- 企業碳風險管理
- AI 與數據策略
- 未來工作場域
- 雲端策略 (雲優先到雲原生)..

串接與導入策略至各營業單位

數位轉型帶來的風險

風險一定會發生，唯有掌握風險者，才能搶得先機

產業生態系管理

專注客戶的需求發展服務，尋找能夠為客戶創造價值的合作夥伴，為企業開啟跨域、跨界的合作契機，在協作過程更新整合數位資源與能力中所才能成一加一大於二的力量。

隱私與資料保護風險

隨著各國對於資料保護之監理要求愈來愈嚴格，在資料分析與應用之過程，應避免觸犯隱私相關法規，同時也要確保採用的資料之品質，才能汲取並創造資料價值。

組織再造與人才發展

培養數位人才與能力，專注於打造數位能力為目標之訓練計畫，以快速取得必要技能，並且能夠基於業務需求， 活化組織的工作能力。同時可考量引進外部人才，與外部商業夥伴，如研發型單位、技術育成 單位或新創公司共同協作，以取得技術、智慧財產、人員等資源為目標，藉以增加組織成長與創新的能力。

新興科技資安風險

駭客經濟旺盛與網路攻擊頻繁，隨著數位化程度的提昇，網路安全風險可能影響的層面也越來越廣，甚至可能影響企業的永續發展。因此，數位轉型的過程中，正視新興科技所帶來的風險，企業才能更自信的掌握風險並管理風險。

供應鏈管理

企業應確保供應商與整體生態圈的網路安全防護等級，包含導入供應鏈的風險評鑑機制，並借力新興科技全面提昇防禦思維，以共同強化防禦力，完善風險控管機制。

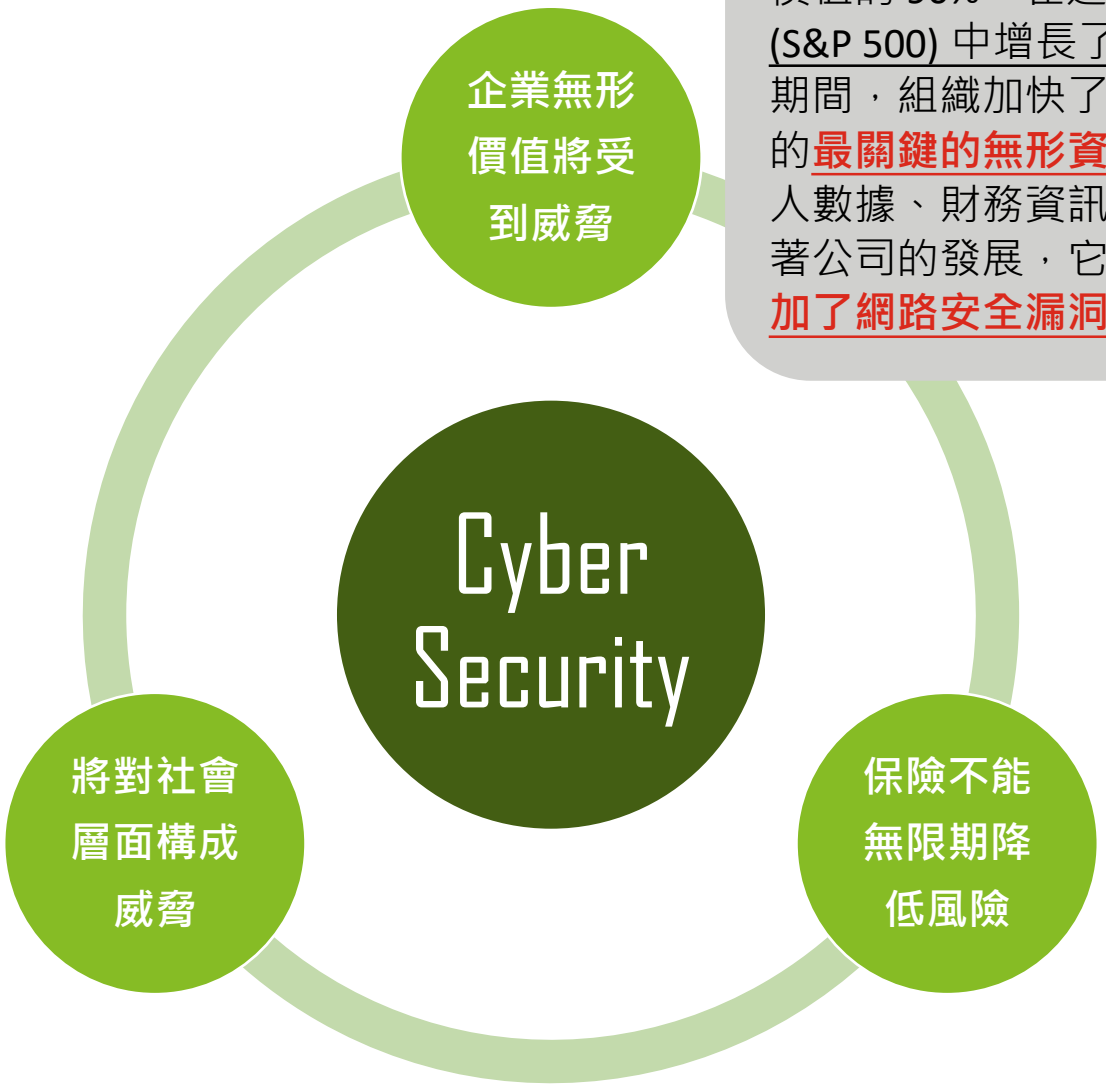
法遵風險

數位時代是一個「網際無邊」時代，法遵風險是產業鏈與生態圈中夥伴的共同責任，企業在法規調合下考量各自權責與分工，並有一套政策及程序來確保組織遵循相關的法律、命令及行政解釋。

為什麼網路安全與資訊安全會是ESG的關鍵問題？

本著消費者便利的精神，各行各業的組織迅速採用了數位化服務交易。這些在政府服務、金融和保險服務、醫療保健和公用事業以及消費品中幾乎無處不在。這會增加資訊安全風險。2021 年，**身份盜竊記錄被打破，比之前的歷史高點增長了 23%**。

數據洩露會對人們產生巨大影響。駭客也逐漸增加針對醫療保健數據和機構的攻擊，對整個社會的醫護服務產生影響。



無形價值為非實體的資產價值，現在佔組織資產價值的 90%，在過去 35 年中在標準普爾 500 指數 (S&P 500) 中增長了兩倍多。在 COVID-19 大流行期間，組織加快了資產數字化的轉變。公司價值的**最關鍵的無形資產可能是資料數據**，無論是個人數據、財務資訊、安全數據還是行為數據。隨著公司的發展，它們的**無形價值也在增長，這增加了網路安全漏洞的潛在影響**。

部分企業沒有實施資訊安全治理，而是依賴保險來管理風險。但若法院持續做出有利於投保人的裁決，保險公司將縮小網絡保單的覆蓋範圍，從而限制組織可以依靠它來降低風險的程度。在任何情況下，**保險索賠都會嚴重影響組織的投保能力；僅靠保險並不能替代資訊安全治理。**

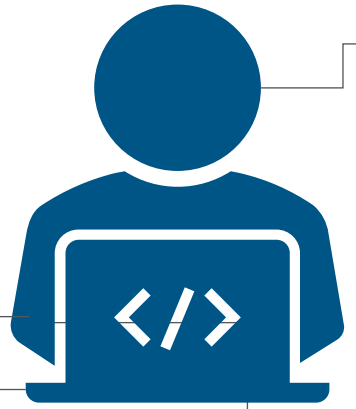
臺灣金融相關產業重大資安事件

花旗銀行

(2022.02)駭客鎖定花旗銀行（CitiBank）用戶，以帳號遭停權、詐騙損害賠償為主旨，吸引用戶連至釣魚網站輸入網銀帳密，以以假亂真的信件，誘使用戶連到釣魚網站輸入帳密或其他個資。

券商APP連線異常因台固、中華電信網路互連斷訊

(2022.06) 台固機房出現異常，造成券商APP下單系統異常。



國泰世華銀行

(2021.10-2022.03)國泰世華銀行因系統升級維護不當，ATM半年當機4次，受影響帳戶數合計3.5萬戶。

(2022.10)因資訊大樓進行電力維護，導致網銀、ATM及信用卡刷卡等功能暫停服務。

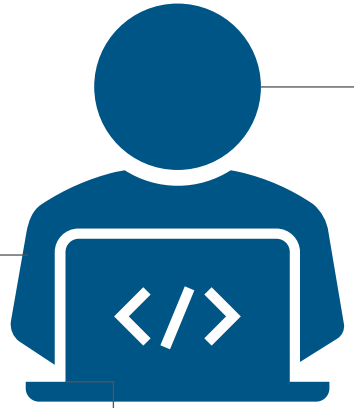
(2022.12)因內部優化系統影響效能，導致用戶登入網銀緩慢，引爆民怨。

永豐銀行

(2023.01) 永豐銀行導入3D驗證機制後，於刷卡時會同時將OTP驗證碼，傳送至持卡人手機及電子郵件信箱，寄送的驗證碼郵件遭到不法人士擷取，所以可以通過3D Secure的驗證，使34名持卡人被盜刷76筆，總金額約110萬元。

全球重大資安攻擊事件

越南大型銀行VPBank NEO
(2023.05)駭客將安卓木馬程式(FluHorse)偽裝成遠通電收ETC、越南大型銀行VPBank NEO的App。攻擊者先是寄送惡意郵件，謊稱收信人要儘速處理付款異常的問題，引誘他們下載帶有FluHorse的冒牌App。



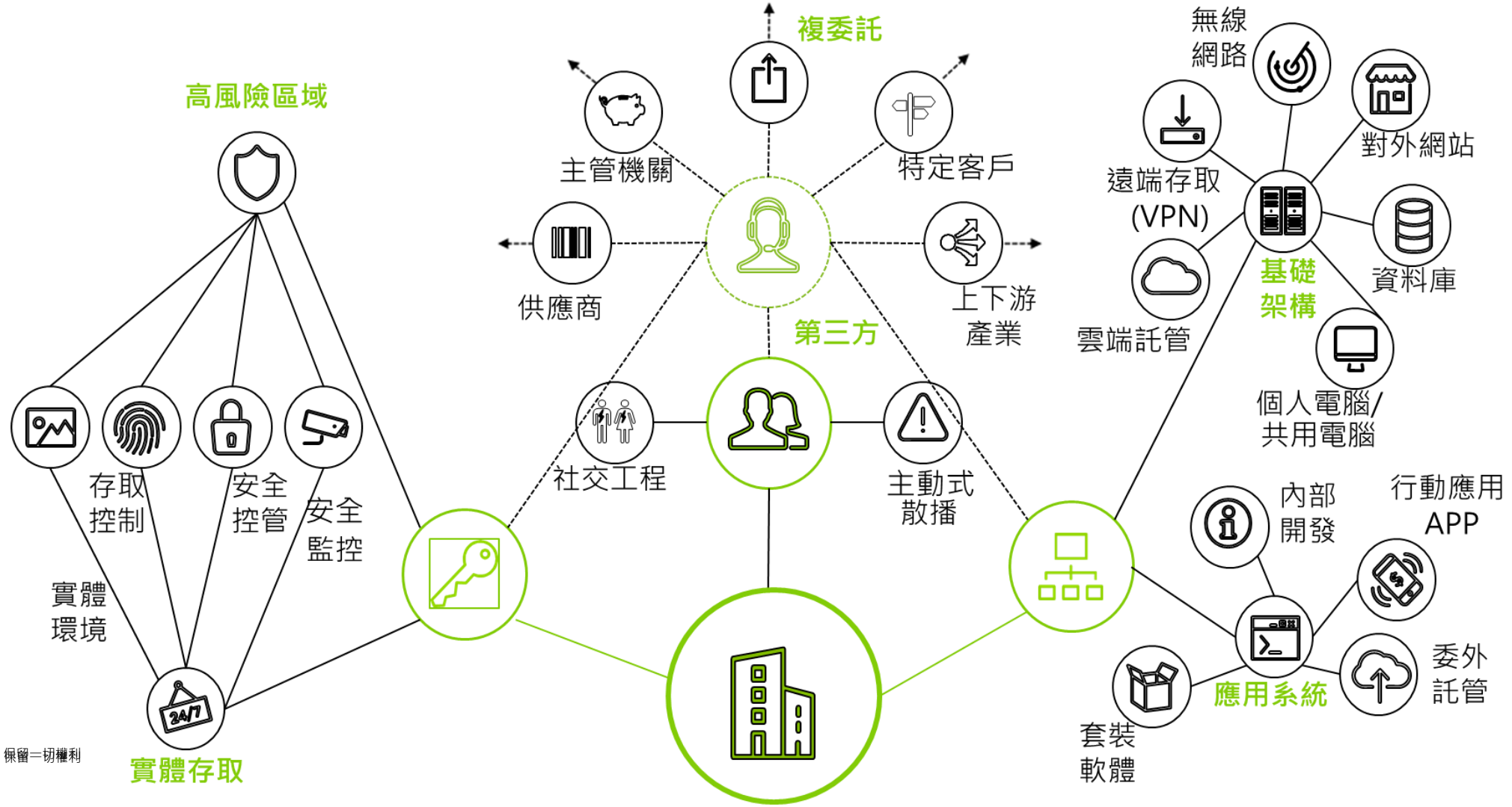
BSI銀行(Bank Syariah Indonesia)
(2022.05)印尼的BSI銀行受到網路攻擊並且被知名勒索軟體組織LockBit竊取1,500萬名客戶或員工之個人資訊(如姓名、手機號碼、地址、帳戶餘額等)，除了ATM 與移動銀行 (m-banking) 服務中斷、遭威脅勒索高達2,000萬美金的贖金外，最終導致1.5TB機敏資訊被公開。

美國矽谷銀行（Silicon Valley Bank）
(2023.03)美國矽谷銀行（Silicon Valley Bank，SVB）宣布倒閉，駭客隨即註冊大量網域，並隨著事態的變化發動多起網路釣魚攻擊。

資安事件可能為企業帶來的損害

找出企業最脆弱的環節加以強化

隨著數位工作方式的變化，以及雲服務的採用、高度連結的供應鏈、更多聯網裝置系統的使用，都暴露新穎且更具挑戰的攻擊面。如果能夠縮減可能遭受威脅的攻擊面，並且強化或修補脆弱的結構，則受到攻擊時將能降低至最小的傷害。



國際標準管理制度控管精神分享

品質管理系統(QMS)的全貌

品質為公司透過態度、行為、流程與活動的產出，可滿足客戶或利害關係人需求與期望的程度，也是一種「組織文化」。所謂「品質好」取決於客戶與利害關係人的感受，公司的產品或服務是否滿足客戶的需求，以及對其他利害關係人產生的影響。

品質管理七項原則

了解顧客的需求與期望；依顧客期望規劃、設計、開發、提供產品/服務；顧客滿意度調查...

依組織願景、策略建立品質政策與目標；溝通品質政策與目標；提供所需資源、訓練、職權...

個人目標與品質目標介接、知識分享與經驗傳承...

管理體系各活動相關串接、影響；各產品/服務活動連結、作業一致，降低重複投入...

針對品質的高風險事項、不合格品、顧客不滿意等項目，持續改善或進行變更...

執行業務過程留存紀錄、訂定績效指標(KPI)與審核執行結果...

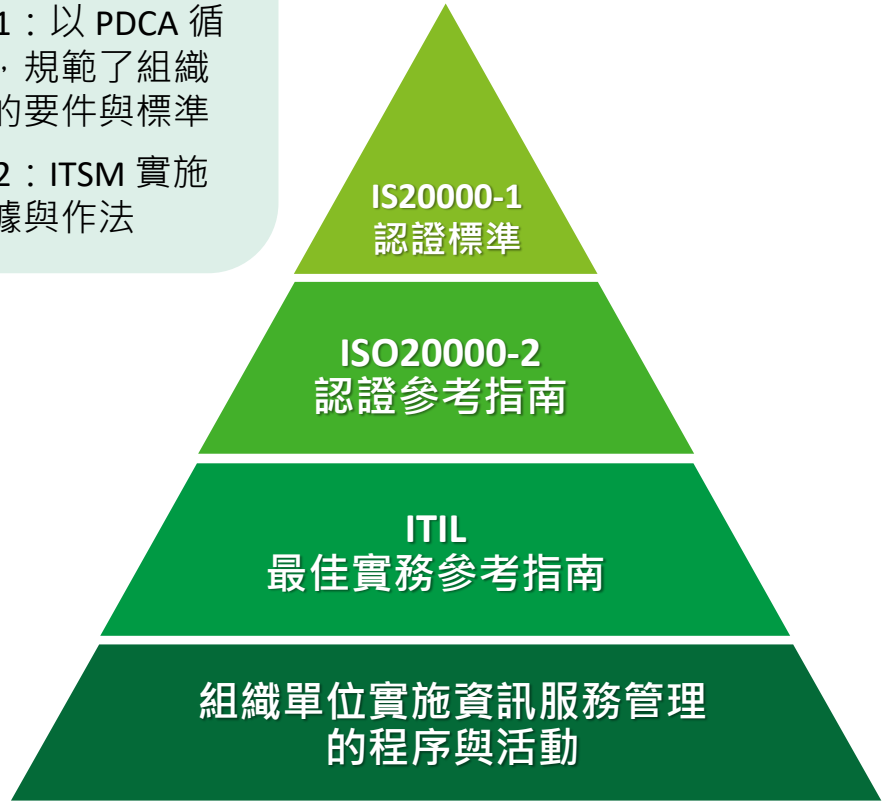
確認組織相關的利害關係人，了解其期望，共享資訊、知識與資源；外部提供者管理...

ISO 20000資訊服務管理 - 基於流程方法之資訊服務管理國際標準介紹

英國政府規劃之ITIL(IT Infrastructure Library)，目前已是全球公認支援資訊服務之最佳實務；ISO 20000係由英國國家標準局(BSi)所發展的資訊服務規範，目前為國際上所最為被認可的「資訊服務管理 IT Service Management, ITSM」標準。

ISO 20000 總共包含二個部份：

- ISO20000-1：以 PDCA 循環為基礎，規範了組織取得認證的要件與標準
- ISO20000-2：ITSM 實施的參考依據與作法



ITIL 4 改版發佈	2019 Q1
ISO20000:2018 改版	2018
ISO20000:2011 改版	2011
ITIL V3 發佈	2007
新制 ISO20000:2005 誕生 (源於BS15000)	2005
修訂ITIL 與 BS15000	2000-2004
CCTA 與OGC (Office for Government Commerce) 合併第一份涉及ITIL的標準被制定出來 : BS15000	2000
ITIL開始於歐洲政府單位與大型企業組織中擴展開來	90年代初
英國CCTA (Central Computer and Telecoms Agency) 組織被付予開發需具有效率且能在財務績效上展現的IT服務之任務	80年代中

資訊服務生命週期

2. End to End 服務管理&新/變更服務之規劃與設計

設計重要服務元件
- 服務目錄/服務水準協議
- IT容量/服務持續性/可用性目標與監控機制
- 資訊安全/委外廠商管理規範

1. 發展IT 服務策略

定義與衡量IT價值
發展重點：
- 財務管理(Finance)
- 組合管理(Portfolio)
- 需求管理 (Demand)

3. IT 服務異動管理

管理服務異動過程對服務運作的影發展重點
- * 組態管理 (CMDB)
- * 變更暨上線部署管理 (建置/測試/評估)

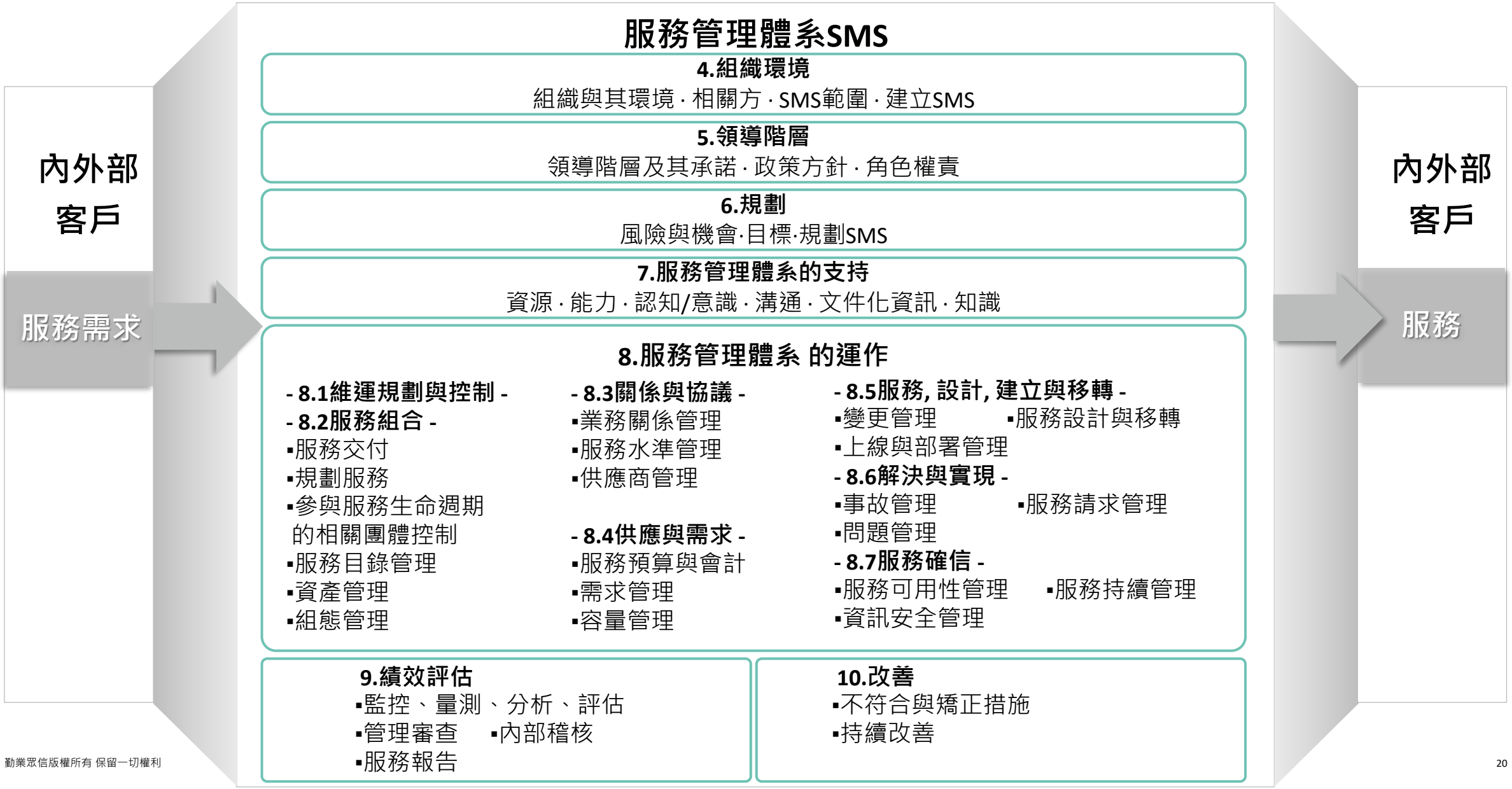
4.服務異常處理與後續問題診斷

管理服務異動過程對服務運作的影響
發展重點：
- 事故管理
- 問題管理
- 請求與存取管理

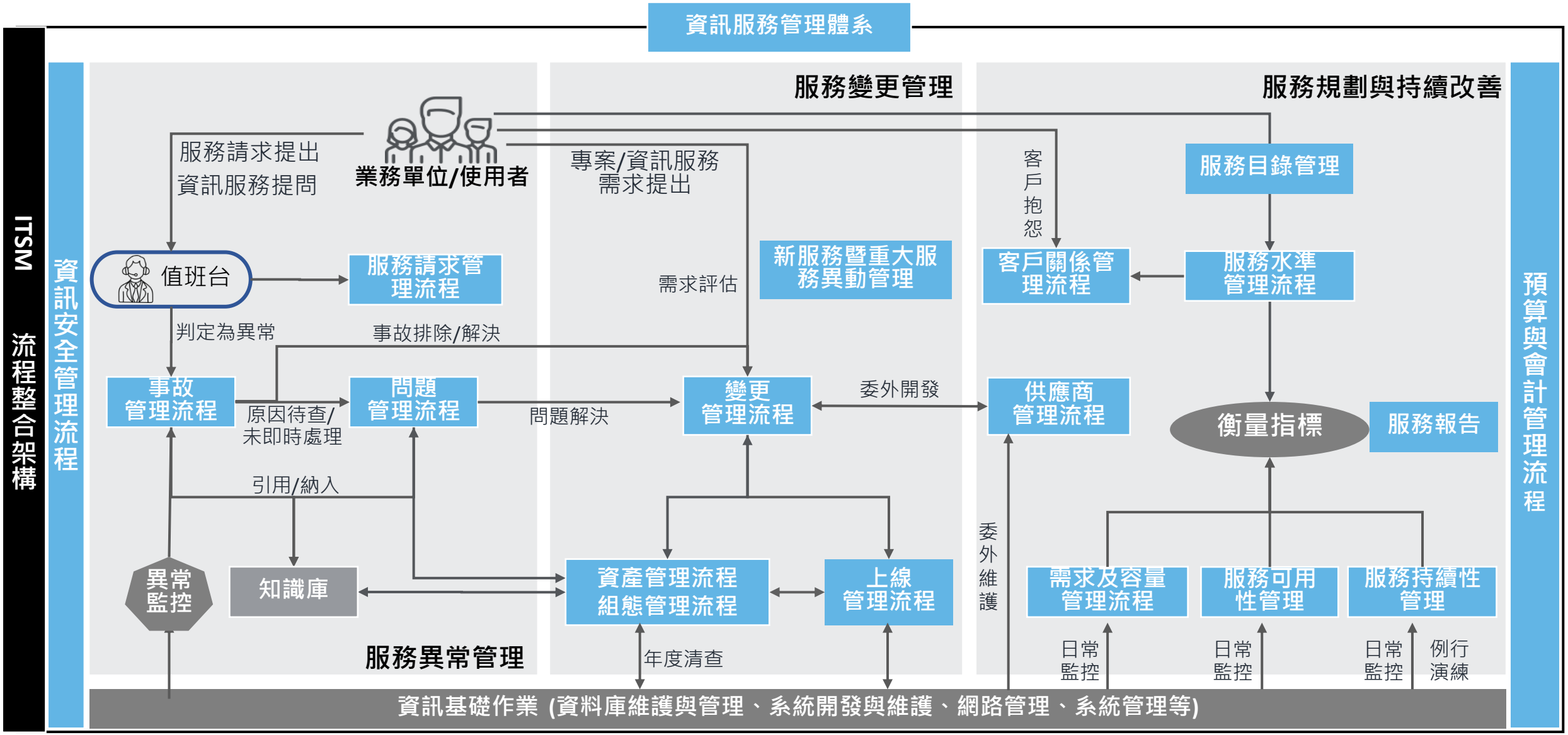
5. IT 服務持續改善

藉由服務報告與KPI監控績效並持續改善服務品質

ISO/IEC20000-1:2018 服務管理體系



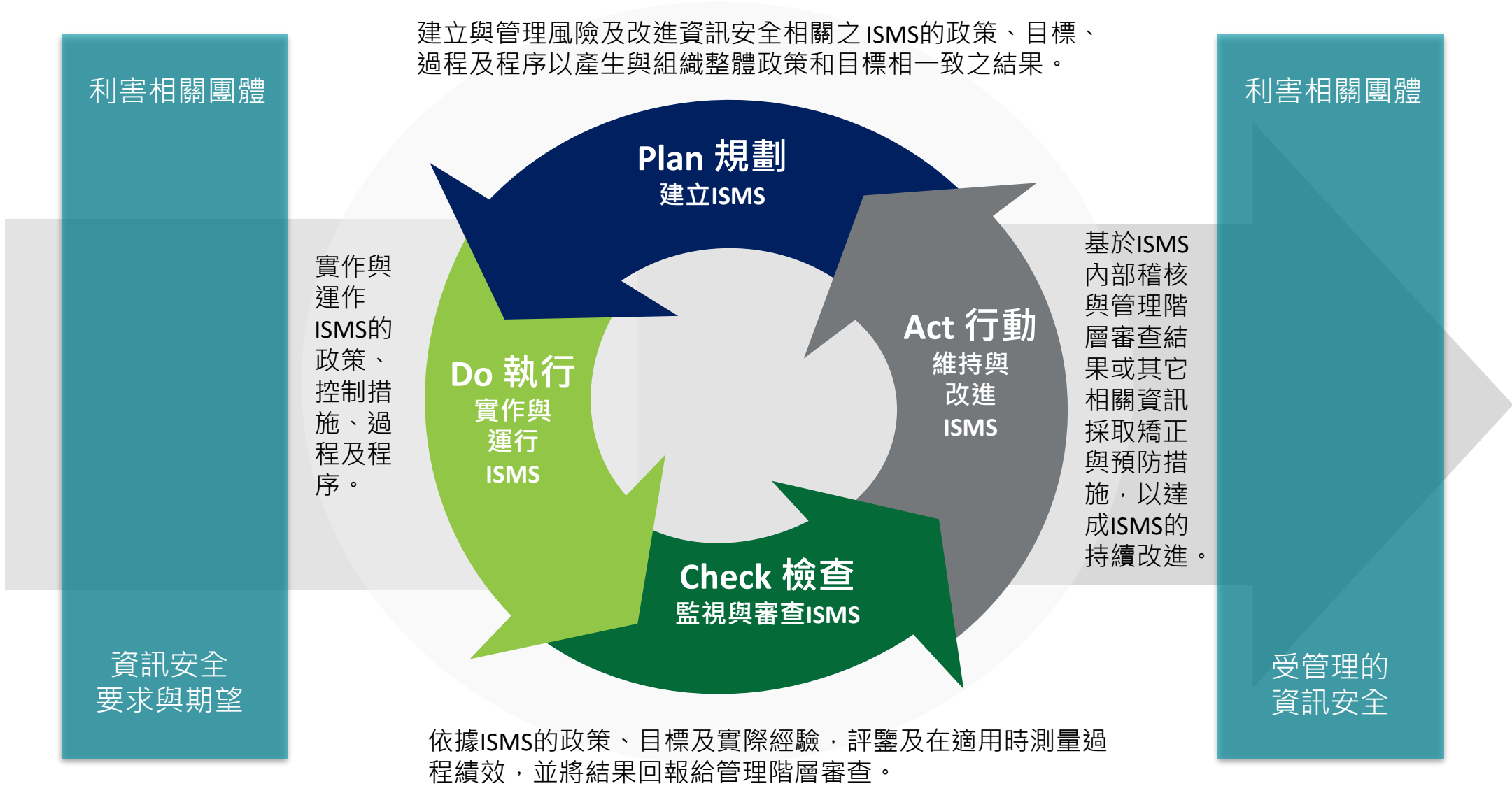
資訊服務管理各流程關聯



資訊安全管理體系簡介

資訊安全管理體系（Information Security Management System，簡稱 ISMS），係針對組織內部所使用之資訊，實施全面性之管理，以妥善保護資訊之機密性、完整性、可用性。

資訊安全管理PDCA過程模式導向(Process Model)



ISO 27001 架構簡介

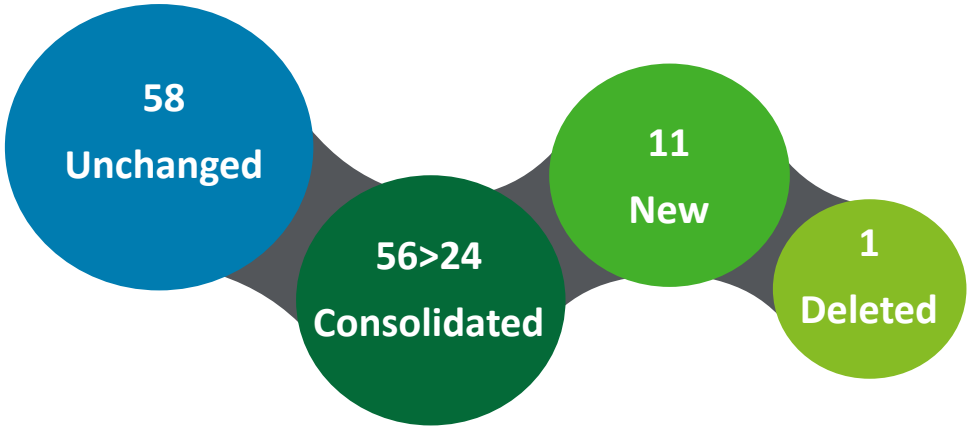
Ch1. 適用範圍(Scope)
Ch2. 引用標準(Normative references)
Ch3. 名詞與定義(Terms and definitions)
CH4. 組織背景(Context of Organization)
Ch5. 領導力(Leadership)
Ch6. 規劃(Planning)
Ch7. 支持(Support)
Ch8. 運作(Operation)
Ch9. 績效評估(Performance evaluation)
Ch10.改善(Improvement)

Certification Standards
為認證的標準

提供資訊安全管理體系(ISMS)之建立實施與文件化之具體要求，依據個別組織的需求，規定要實施之安全控制措施的要求，不是技術標準，而是管理標準。

附錄A. 控制目標與控制措施

- 5. 組織控制 Organizational
- 6. 人員控制 People
- 7. 實體控制 Physical
- 8. 技術控制 Technological



4 大控制主題　**93** 項控制措施

可依據組織業務
選擇適用的管控要求

ISO 27002主要是作為參考文件，提供廣泛性的安全控制措施，作為現行資訊安全之最佳實務與作業方法，不作為評鑑與驗證標準。

新版草案從原114個控制措施調整為93個控制措施，整體數量雖然下降，但主要原因是將原有控制措施進行整併，並且針對編號進行進行適當調整，轉版重點應特別針對新增條款進行評估確認。

ISO 27002 控制措施異動說明

原2013版刪除　原2013版內容　新增內容

組織 (5.1 ~ 5.37)

- 5. 資訊安全政策
- 6.1 內部組織
- 威脅情資
- 7.2.1 管理階層責任
- 8. 資產管理(除8.3)
- 9.1 存取控制要求事項
- 9.2 存取管理 (除9.2.3)
- 9.3 使用者責任
- 9.4.3 通行碼管理
- 12.1.1 文件化
- 14.1.1 資訊安全要求與規格
- 15. 供應商管理
- 使用雲端服務的資訊安全
- 16. 資訊安全事件管理 (除16.1.2、16.1.3)
- 17.1 資訊安全持續管理
- 為業務連續性做好ICT準備
- 18. 遵循性 (除18.2.3)

人員 (6.1 ~ 6.8)

- 6.2.2 遠距工作
- 7. 人力資源安全 (除7.2.1)
- 13.2.4 機密性或保密協議
- 16.1.2、16.1.3 事件/弱點通報

實體 (7.1 ~ 7.14)

- 8.3 媒體處置
- 11. 實體及環境安全 (除11.2.5)
- 實體安全監控

刪除

11.2.5 資產之攜出
(相關內容並非完全刪除，分別涵蓋於新版本7.9 場外資產安全、8.10 訊息刪除條款中)

技術 (8.1 ~ 8.34)

- 6.2.1 行動裝置政策
- 9.2.3具特殊存取權限之管理
- 9.4系統及應用存取控制 (除9.4.3)
- 10. 密碼學
- 12. 運作安全 (除12.1.1)
- 18.2.3 技術遵循性審查
- 配置管理
- 訊息刪除
- 數據遮罩
- 防止數據洩露
- 監測活動
- 13. 通訊安全 (除13.2.4)
- 網頁過濾
- 14. 系統開發及維護 (除14.1.1)
- 安全編碼
- 17.2 多重備援

ISO 27701目標

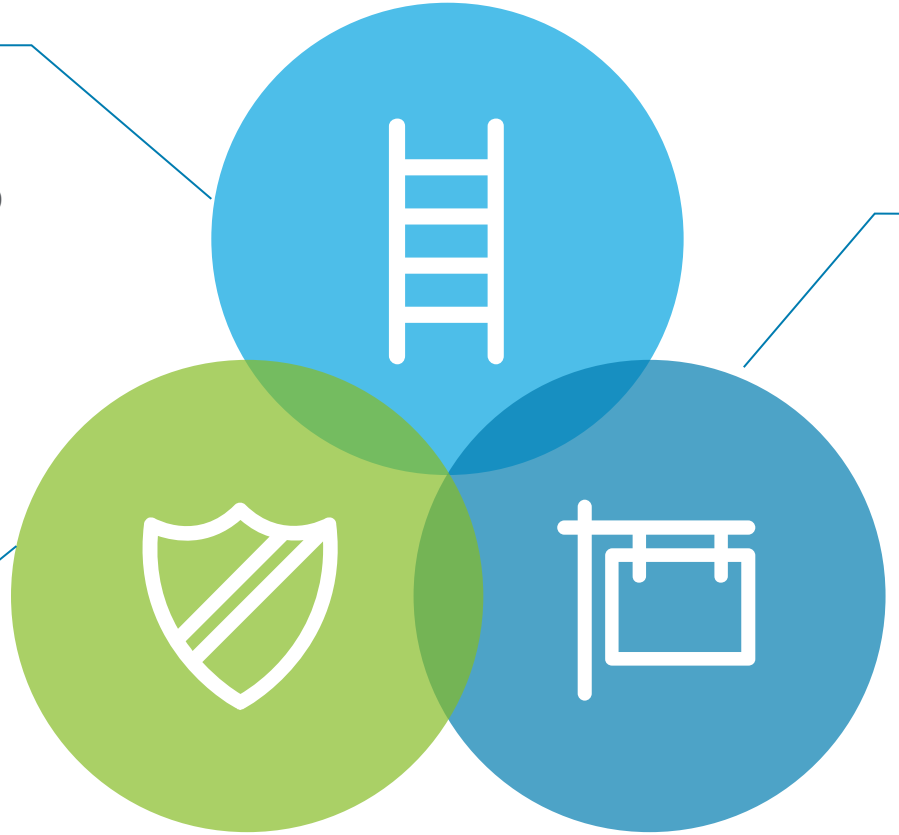
通過對於隱私保護的控制實現對ISMS進行補充，使企業建立PIMS，實現有效的隱私管理，從而使企業獲益。

明確隱私保護管理合規目標

通過明確對 PII 控制者和處理者的隱私保護要求，**減輕企業合規負擔的同時降低企業合規風險**， ISO 27701 標準附件D中明確表示，單個隱私控制點可以滿足 GDPR 中的多項要求。

實現持續安全治理的課題

通過建立PIMS，可以確保組織高級管理層、企業所有者以及關鍵相關方的利益滿足隱私保護要求，從而使組織實現**長期、持久的個人隱私安全合規**。



向企業客戶或合作夥伴傳達隱私合規價值

PII控制者通常會要求PII處理者提供相關證據，從而證明PII處理者的隱私管理體系符合適用的隱私管理要求。**通過得到授權的協力廠商機構對PII處理者進行審計驗證**，基於國際標準的統一證據框架可以極大地**降低合規溝通成本**，這種合規透明度的提高對於企業戰略和業務決策至關重要，同時PIMS認證也有助於**向公眾傳達企業的可信度**。

ISO27001與ISO27701重點比較

管理系統框架要求	ISO27001:2013	ISO27701:2019
	資訊安全管理制度	個人資訊管理體系管理制度
重點	ISO27701以ISO27001的框架為基礎，增加隱私資訊要求項目的要求，並更加著重於可識別個人資料Personally Identifiable Information(PII) 的控管。ISO27701的條文要求基礎以ISO27001為底，針對隱私資訊要求的部分則會做相對應的補充及新增要求、條款及附錄。	
	本文條款: 1-10	本文條款: 1-5 (新增要求)
	控制項目: A5-A18	控制項目: 6.2-6.15 (新增要求)
	N/A	7.1-7.5 對PII**控制者**的附加指引, Annex A 8.1-8.5 對PII**處理者**的附加指引, Annex B (新增條文、附錄)

PII控制者	PII處理者
指單獨或與他人共同決定個人資料處理之目的之組織， 需規範處理者依控制者要求保護個資，如於合約中訂定相關要求。可能有不只一個組織為控制者時，則為PII共同控制者。	指受控制者委託處理個資料之組織需確認是否依與控制者訂定之契管控及保護相關個資。

ISO/IEC 27701標準重點解讀

ISO 27701擴展了ISO 27001的要求，在原有的管理、實施、操作、監控、審查和不斷改進ISMS的流程基礎上，著重考慮了對於企業所持有PII的隱私保護。

ISO 27701

對 ISO 27001擴充要求	對 ISO 27002擴充要求	針對PII控制者之額外指導	針對PII處理者之額外指導
• 組織環境 • 領導 • 規劃 • 支援 • 運作 • 績效評估 • 改善	• 資訊安全政策 • 資訊安全組織 • 人力資源安全 • 資產管理 • 存取控制 • 加密 • 實體與環境安全 • 作業管理 • 通訊管理 • 系統取得、開發與維護 • 供應商關係 • 資訊安全事故管理 • 營運持續管理 • 遵循性	• 蒐集與處理 PII 之條件 • 對 PII 主體之義務 • Privacy by design and privacy by default • PII 共用、移轉與披露	• 蒐集與處理 PII 之條件 • 對 PII 主體之義務 • Privacy by design and privacy by default • PII 分享、傳輸與揭露

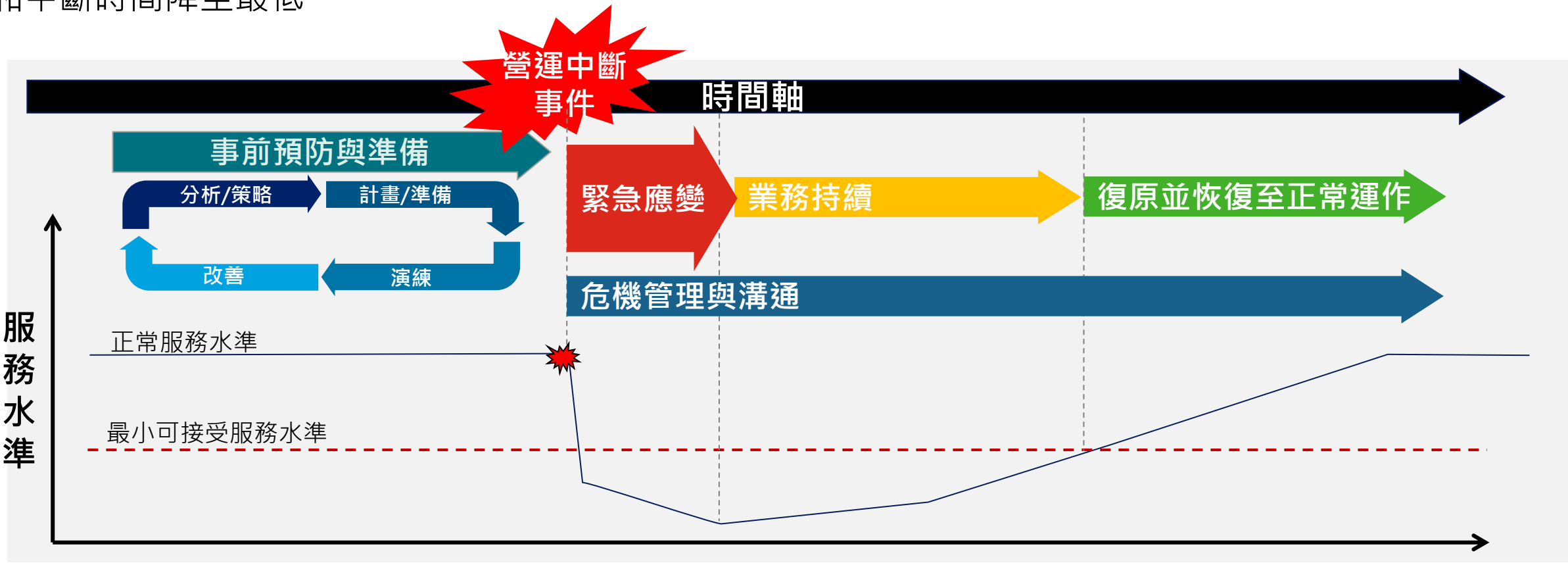
- PII: Personally Identifiable Information 個人可識別資訊

關於營運持續管理(Business Continuity Management, BCM)

居安思危 – 以最有效益的資源配置，建立因應及復原能力。

協助企業正視風險，展現企業對於持續營運及提供服務的承諾。

藉由實施**營運持續管理作業**，將重大實體災害（如地震、火災）或資訊服務故障事件時所帶來的衝擊和中斷時間降至最低。



什麼是營運持續?

地震

火災

電力中斷

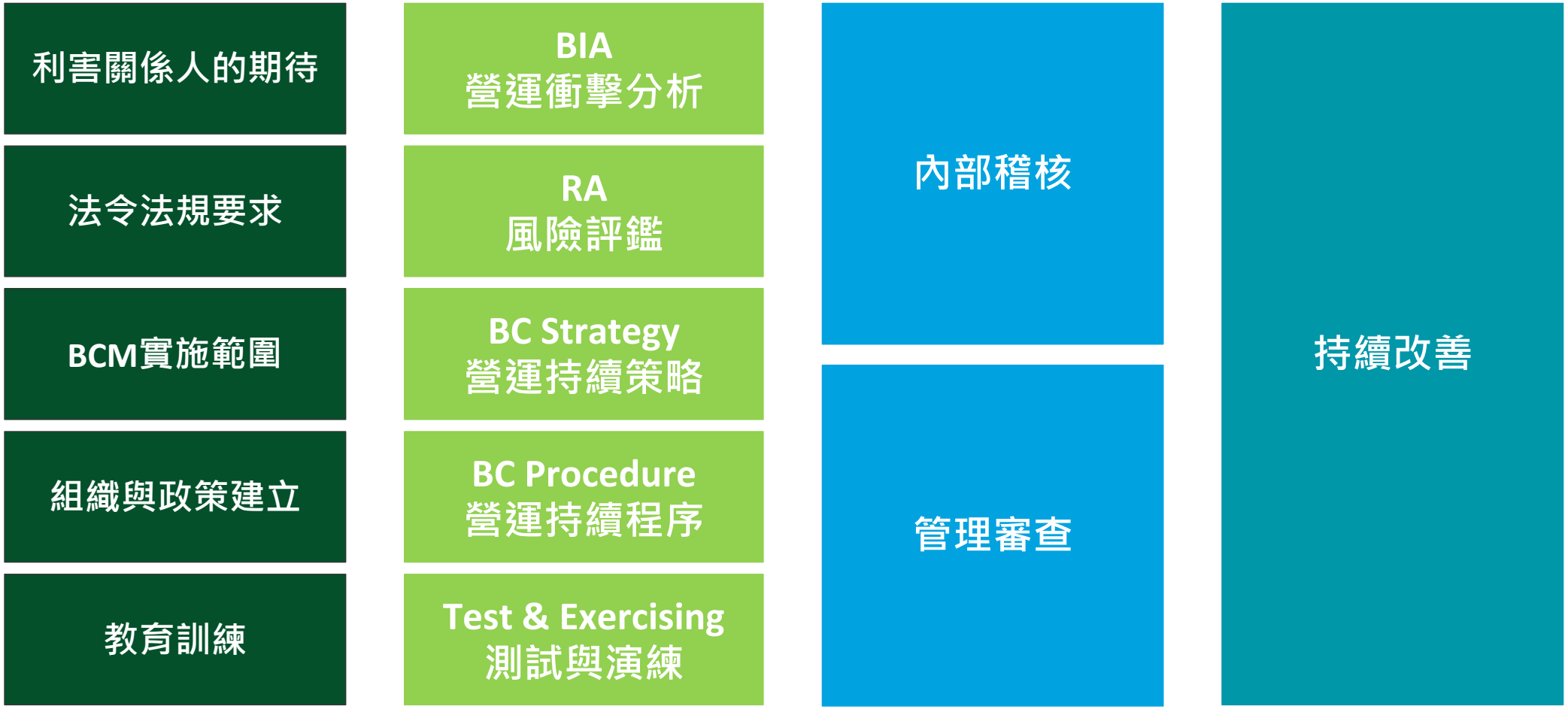
資訊系統故障

當發生災害且造成嚴重的災損

公司關鍵業務因此中斷時

能透過一套有效的方式，
盡速回復關鍵業務

營運持續管理工作要項



營運持續管理重點活動

國際標準管理制度導入效益

金融機構主管機關對於資訊安全、個資管理與營運持續管理之期待

ISMS　ISMS + PIMS　BCMS

自我要求 → 主管機關鼓勵 → 合規要求

金融金融資安行動方案2.0

✓ **5.1推動金融機構導入國際資安管理標準**

規劃請相關公會依業別特性，訂定**各業別國際資安管理標準驗證之範圍**，並**推動一定規模或電子交易達一定比例之金融機構導入國際資安管理標準及取得驗證。**

✓ **8.2鼓勵金融機構導入國際營運持續管理標準**

鼓勵金融機構**導入國際營運持續管理標準**，參採最佳實務做法，並透過第三方獨立機構驗證符合來自內部、法規、及客戶的各種要求，並據以向利害關係人溝通其面臨衝擊之準備。

金融機構資通系統與服務供應鏈風險管理規範

第六條 供應商之委託契約或相關文件中，應明確約定下列事項：

一、要求供應商遵守相關法令法規及**其他適當資訊安全國際標準要求**，並訂定供應商未符合資訊安全要求或服務水準時之罰責標準。

金融機構主管機關對於資訊安全、個資管理與營運持續管理之期待

ISMS　ISMS + PIMS　BCMS

建立證券商資通安全檢查機制
建立期貨商資通安全檢查機制

- 應依其所屬資安分級辦理核心系統導入**資訊安全管理系統**，並**通過公正第三方之驗證，且持續維持驗證有效性**。

建立期貨商資通安全檢查機制
中華民國期貨業商業同業公會供應鏈風險管理自律規範
中華民國證券商業同業公會供應鏈風險管理自律規範
證券投資信託事業證券投資顧問事業供應鏈風險管理自律規範
證券暨期貨市場各服務事業供應鏈風險管理參考指引

- 資訊服務供應商應具備完善之資通安全管理措施或**通過第三方驗證**。

證券暨期貨市場各服務事業資訊作業韌性參考指引

- 資訊服務供應商應具備完善之資通安全管理措施或**通過第三方驗證**。

金融機構主管機關對於資訊安全、個資管理與營運持續管理之期待

ISMS　ISMS + PIMS　BCMS

- ✓ 保險業辦理電子商務應注意事項
- ✓ 保險業辦理遠距投保及保險服務業務應注意事項
- ✓ 保險業申請業務試辦作業要點

- 保險業辦理電子商務、遠距投保及保險服務業務，應**取得資訊安全管理系統國際標準認證（ISO27001）、個人資料管理系統（PIMS）**之認證。
-)試辦業務項目之保險業及委外合作廠商倘涉及蒐集、處理、利用個人資料，應取得**資訊安全管理系統國際標準（ISO27001）、個人資料管理系統（PIMS）之驗證**。

- ✓ 保險代理人公司保險經紀人公司辦理網路投保業務及網路保險服務管理辦法
- ✓ 保險代理人公司保險經紀人公司辦理遠距投保及保險服務業務應注意事項

- 保經代公司申請辦理網路投保業務，應符合取得**資訊安全管理系統國際標準（ISO 27001）之驗證**，及建立防禦網路分散式阻斷服務攻擊（DDoS）之網路流量清洗機制者。
- 保經代公司辦理遠距投保及保險服務業務至少應取得**資訊安全管理系統國際標準（ISO27001）、個人資料管理系統（PIMS）之驗證**。

台灣金融機構管理制度推動 - 112年度金融檢查重點

金融機構主管機關近年也將資訊安全、個資保護與營運持續等管理要求納入金融檢查之重點。

金融控股公司

- **風險管理機制**：對國際金融情勢變化，是否預擬因應對策及建立集團風險管理機制，如：營運持續管理計畫、壓力測試等。
- 督導並檢視各子公司對更新資訊系統相關規劃作業之妥適性(如：系統轉換穩定性及測試作業)、網路系統安全控管及資訊安全維護，建立有效之偵測及防護措施，及建置網路系統發生異常時之緊急應變作業程序、復原計畫及客戶權益保護機制。
- **個人資料保護**：金控公司及其子公司建置客戶資料庫之資訊安全管控及個人資料蒐集、處理及利用之安全維護措施、個資外洩應變演練機制、共同行銷之安全維護措施及法令遵循情形、辦理金融機構間資料共享，是否依循個人資料保護法及金融機構間資料共享指引等規定辦理，建立妥適內部控制規範及資訊安全落實情形。

本國銀行

- **資通安全管理**：如資安專責單位與專責主管之職能發揮(含指派副總經理以上或職責相當之人兼任資訊安全長)、防範主機系統及程式異常控管措施(如系統架構重大變更之資安控管、完整測試、程式源碼檢視)、個資檔案之儲存、傳遞與存取控管機制【含數位服務個人化(MyData)服務平台之資訊安全管控機制】、網路安全措施(如防火牆與入侵偵測、弱點掃描及滲透測試等資安防禦措施暨漏洞修補改善、物聯網設備管理、資安事件監控與通報處理)、供應鏈風險管理(如對受託廠商監督、交付系統及元件安全檢測、合約妥適性)。

證券業

- **風險管理機制**：對疫情衝擊、全球政經情勢變化及升息環境所產生市場風險是否擬定因應對策；是否訂定持續營運管理規範並落實執行；審視風險管理機制運作是否妥適(如董事會與經營層監督管理、風險管理委員會、限額管理、停損管理及例外處理機制等)。

證券投資信託公司

- **資通安全管理之執行情形：**
- 個人資料保護：如個人資料檔案儲存、處理及傳遞之安全維護措施及金融機構間資料共享辦理情形。
- 對金融資安資訊分享與分析中心(F-ISAC)所公布之資安情資或警訊來源之處理情形。

國際標準管理制度導入效益

增強企業資訊安全能力

協助企業建立完善的資訊安全管理機制，包括資訊安全政策、風險管理、資訊安全控制、安全事件管理等。這些措施能夠有效提升企業的資訊安全能力，降低遭受資安攻擊和資料外洩的風險。

保護資訊資產

資訊安全管理制度提供了全面性和系統性的方法來管理和保護企業的資訊資產，減少資訊外洩、損壞和損失的風險。

供應鏈管理

與利害關係人合作，管控整個企業和供應鏈中的風險，助於企業避免產生或減少營運中斷的成本、風險與損害。

持續改進

導入國際標準制度，讓企業能以P-D-C-A循環持續強化內部管理制度要求。

提升企業聲譽和競爭力

導入國際標準制度，能夠提升企業的信譽度和公信力。同時，因為更多的企業和機構要求其供應商實施國際標準管理要求，導入國際標準制度也能夠提高企業在競爭市場中的競爭力。

合規要求

許多國家和地區的法律法規都要求企業保護客戶和員工的敏感資訊。導入國際標準制度能夠幫助企業遵守相關的法律法規和合規要求，減少違反法規的風險和懲罰。

提升生產力

標準化的服務流程，減少不確定性及耗時的溝通。

正面管理，主動出擊

企業主動出擊，及早擬定資安控制，防護、監控與應變之機制，得減低突發事件對企業造成的衝擊。

國際標準管理制度整合方法論

國際標準管理制度架構相同，故不同的制度導入得以統一一套體系作業進行整合，以達到多面向的安全管理要求。

	ISO 9001	ISO 27701 /PIMS	ISO 27001/ISMS	ISO 20000	ISO 22301/BCM	體系活動整合
管理目標	品質管理目標	個資管理目標	資訊安全目標	服務目標、SLA及服務報告	服務等級管理	績效指標整合
	品質管理有效性量測		資訊安全控管有效性量測	SLA		
資產收集及風險識別	品質管理風險識別	個資衝擊分析	資訊安全風險評鑑及系統開發	變更與上線部署	BIA/RA	變更上線整合
		個資風險評鑑	資訊資產蒐集與管理	資產組態管理	IT RTO　人工 RTO	資產與組態整合
日常作業應變	品質事故管理	個資事故管理	資安事故通報	事故管理	備援規劃	資安事件與營運持續管理整合
				服務持續性管理	啟動備援機制	
關係管理	第三方品質管理	第三方管理	第三方安全管理	客戶關係管理	下包供應商之BCM配合事項	客戶及供應商管理整合
				供應商管理		

意見交流

Deloitte.

勤業眾信

Deloitte.

勤業眾信

資安防護下的數位身分驗證

臺灣網路認證公司

TWCA 臺灣網路認證

TWID 身分識別中心

大綱

1. 資安事件頻傳
2. 證券客戶身分之資通防護規範
3. 資安防護下的數位身分驗證方案
   - MID KYC
   - MID 企業門號確認
   - 撞庫強化
   - 零信任
   - 網站實名

委外廠商管理不當造成個資外洩

NEWS

微笑單車官網遭受境外 IP 網路攻擊

微笑單車官方網站於2023/5/17遭到駭客網路攻擊，發現有境外IP嘗試取得會員帳號與密碼的情況。

YouBike微笑單車遭駭客侵入，導致2.1萬會員資料恐被竊取，為了彌補會員，微笑單車26日也公布最新補償方案！微笑單車表示，**補償方案為提供相關會員每人500元之YouBike 2.0 騎乘券，目前騎乘券機制已進行開發中，將於112年9月份可上線使用**。

微笑單車 action

- 微笑單車已通報政府相關主管機關及提供資訊予檢調單位進行調查，並同步依照ISO27001及BS 10012個資管理標準，進行全面系統潛在風險盤查，避免再發生。

一. 提升密碼強度，並定期變更密碼；
二. 留意會員帳戶內資料是否正確，以及是否有不明卡片與異常騎乘記錄；
三. 若收到不明的來電、EMAIL或簡訊要求匯款或轉帳，請不要開啟或點擊網址連結；若有欠費，請勿匯款，請至車機、車柱或服務中心辦理繳納。若對資訊有任何疑問，歡迎撥打YouBike客服電話進行確認，本公司客服人員將竭誠為您服務。

資料出處:數位時代,https://www.bnext.com.tw/article/75330/youbike-cyber-security ,2023/6/30擷取

單一企業個資事故恐造成連鎖效應

NEWS

電子發票平台資安爆漏洞 逾 7% 上市櫃公司營業隱私恐外洩

READr 近日接獲民眾提供一份包含 130 家上市櫃公司的名單，指稱財政部負責的「電子發票整合服務平台」登入系統出現資安缺失：只要輸入名單上企業的統編，以及政府提供的預設密碼，即可瀏覽其會員資料。也就是說，**只需使用同一組密碼，包括發票明細、營業收入等企業經營之重大商業資料將一覽無遺**。

根據此份名單，1789 間上市上櫃公司中就有超過 7% 的企業仍沿用政府提供的預設密碼，其中 78 間為上市公司、52 間為上櫃公司。從產業別來看，光電業最多，其次是半導體業、電子零組件業，甚至連專門從事資訊安全的公司也榜上有名...。

資料來源：鏡周刊，
https://www.mirrormedia.mg/story/20230516readr001/ (2023.5)

財政部 action

- 整合服務平台營利事業密碼弱點已改善完成
- 推動新版「**雙認證模式**」。以舊預設密碼登入後即強制變更密碼，並應輸入第二因子，始得使用整合服務平台服務

《take away》

1. 資安、個資保護政策，需要落實於產品、服務流程
2. 客戶完成Onboarding後，後續登入應留意身分驗證機制具備可信賴度
3. 最後，安全風險無法一勞永逸，新興科技、犯罪手法衍生之風險議題，應定期、不定期分析及因應

電商網站個資頻傳

蝦皮購物　誠品書店 elite bookstore

NEWS

蝦皮,誠品個資外洩未改善遭罰款

蝦皮、誠品生活及旋轉拍賣等業者涉及消

蝦皮對委外廠商未落實稽核，未能提供完整的安全管控執行、稽核紀錄等具體佐證資料，無法證實該公司對保有個資已採行適當之安全措施，因此依據《個資法》第48條第4款併第50條規定，處分業者併同其負責人罰鍰計新臺幣20萬元。

誠品生活案，經數位部產業署實地行政檢查，現場已發現在帳號管理上執行未確實，另要求事後提供之補充或佐證資料，該公司個資盤點資料仍不完整，且針對委外廠商監督管理未落實執行，因此依據個資法第48條第4款併第50條規定處分，業者併同其負責人罰鍰計新臺幣10萬元。

數位發展部

已要求前述業者落實個資法相關規定，並限期請業者再為改正，如屆期未改正，將按次處分。同時數位部要求各電商業者務必重視個資保護，並且數位部也會引入相關解決方案例如隱碼技術，與電商業者合作，持續強化個資保護措施。

資料出處:數位時代，https://www.bnext.com.tw/article/74423/shopee-data-breach, 2023/6/30 擷取

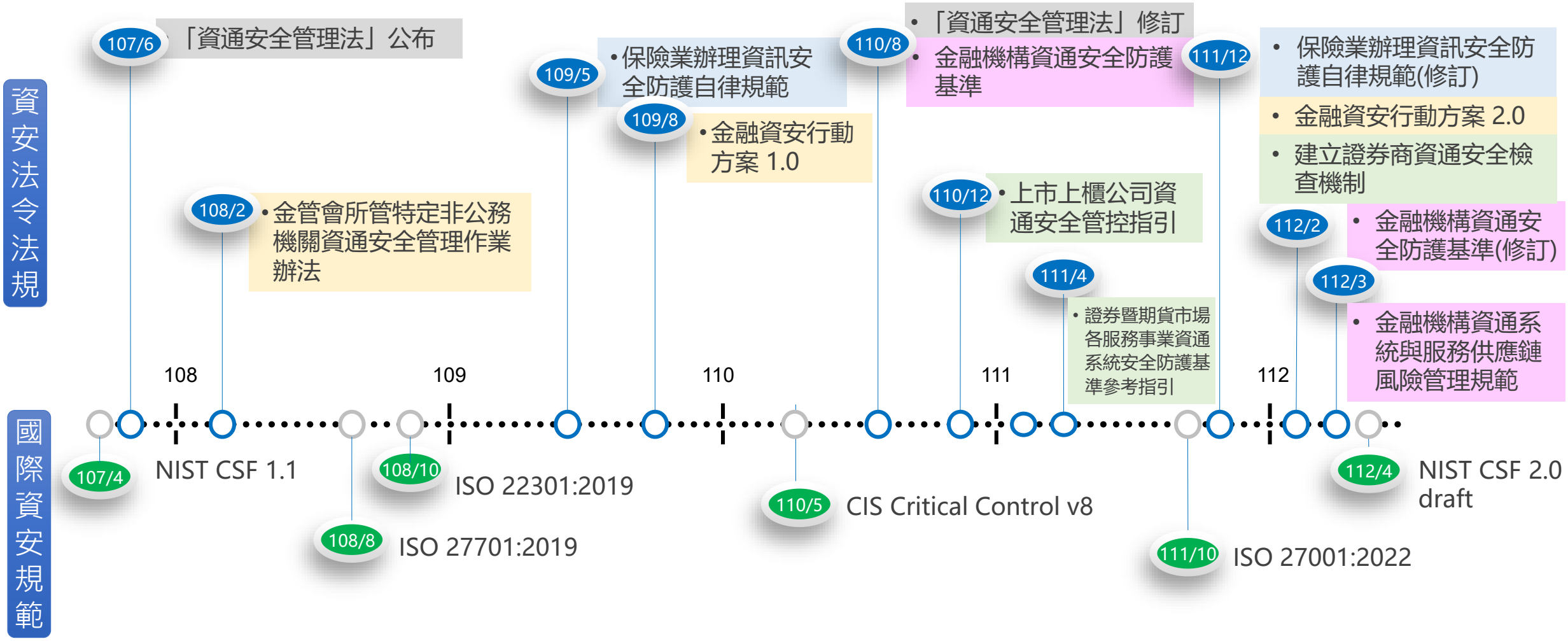
近期資通安全事件解析 - 1

新聞事例	資通安全 風險	資通安全要求 關鍵議題	企業管控措施 可強化方向
微笑單車公司 「YouBike」	「YouBike」系統遭境外及境內網路攻擊，致約有4萬多名會員交易的資料，包含手機號碼、密碼、卡號及交易資料可能遭竊取	委外	第29條 1. 訂定資訊作業委外安全管理程序，包含委外選商、監督管理(如：對供應商與合作夥伴進行稽核)及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。 第30條 1. 訂定委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協議(SLA)、資安要求及對委外廠商資安稽核權
		開發安全	第13條 1. 將資安要求納入資通系統開發及維護需求規格，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。 第16條 1. 對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。 a.定期辦理弱點掃描。 b.定期辦理滲透測試。 c.系統上線前執行源碼掃描安全檢測。
財政部 發票平台	財政部發票平台爆資安漏洞，只要輸入企業統編、政府提供之預設密碼，就可以瀏覽器超過130家上市櫃公司資料，甚至包含國營事業及國安單位的採購資訊	存取控制、身分驗證管理	第21條 1. 建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。

近期資通安全事件解析 - 2

新聞事例	資通安全風險	資通安全要求關鍵議題	企業管控措施可強化方向
蝦皮、誠品生活	蝦皮、誠品生活未依照個資法採取適當資安措施，遭數位部開鍘各罰20萬、10萬	個資盤點、風險評估	第11條 1. 定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。 第12條 1. 定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等
		資通安全防護及控制及監控	第18條 1. 具備下列資安防護控制措施： a. 防毒軟體。 b. 網路防火牆。 c. 如有郵件伺服器者，具備電子郵件過濾機制。 d. 入侵偵測及防禦機制。 e. 如有對外服務之核心資通系統者，具備應用程式防火牆。 f. 進階持續性威脅攻擊防禦措施。 g. 資通安全威脅偵測管理機制(SOC) 第19條 1. 針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。 2. 建立資通系統及相關設備適當之監控措施，如：身分驗證失敗、存取資源失敗重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。

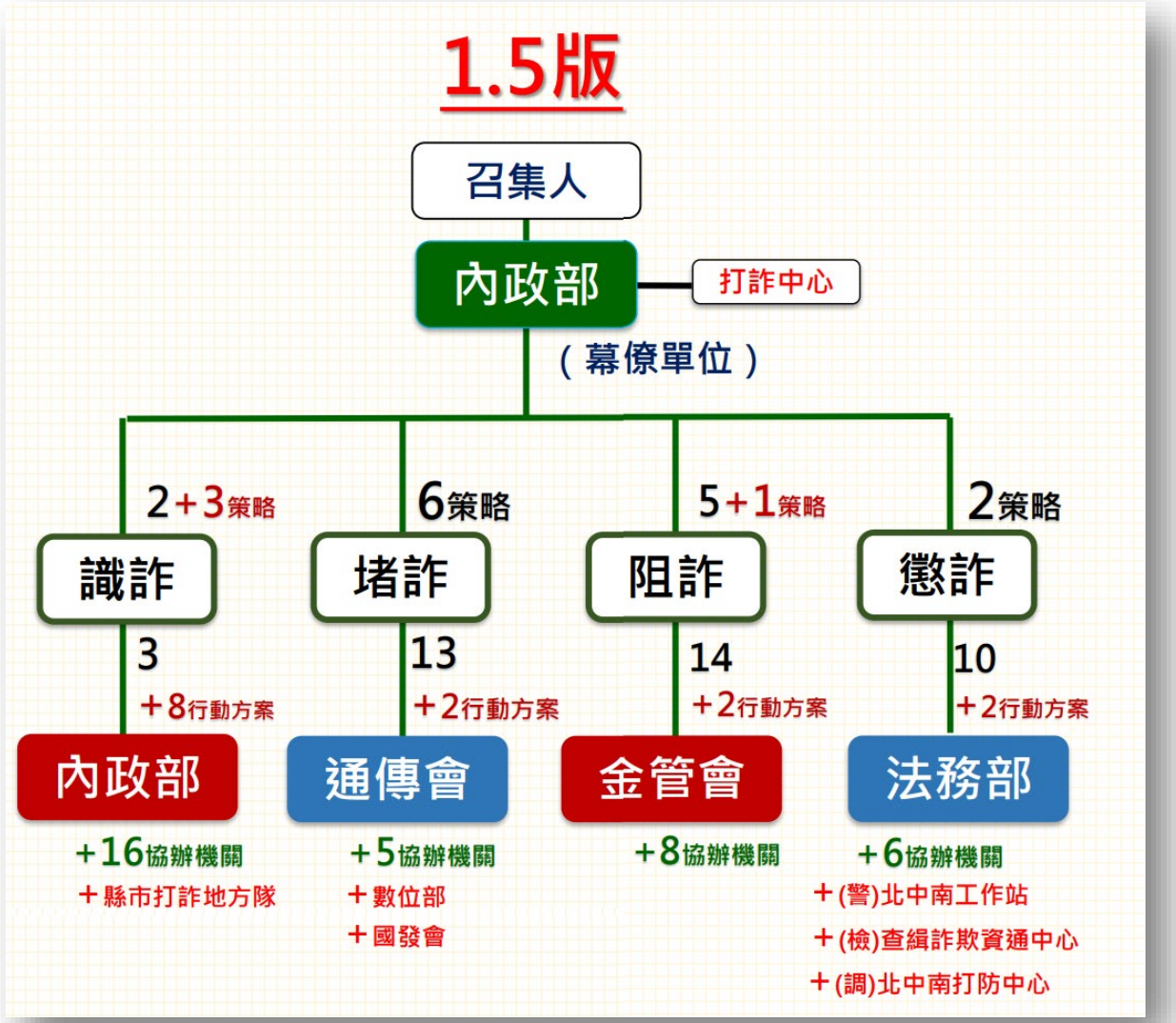
金融資通安全環境逐步成熟



資通科技發展導致詐欺樣貌多樣化

資通科技詐欺用途	特性	常見詐騙手法	詐術施行技術含量	共通點
詐欺工具	針對特定受害人，利用資通工具使本人違反其意願為匯款等行為。	如，社交工程、勒索病毒	高	客戶資料(直接/間接個資、或營業等資料)外洩，為詐欺集團用於不法用途。
詐欺場所	面對不特定一般人，以名人冒名、假網站等詐術使人交付本人或第三人財產。	如，假投資、一頁式詐騙	低	
詐欺客體	針對目標系統或網路進行惡意攻擊，以影響目標對象服務可用性。	如，網頁替換	中	

政府四路打詐，以增加 詐欺成本 為行動目標



- 2022年7月15日行政院訂頒「新世代打擊詐欺策略行動綱領」，由內政部主責

- 2023年5月14日政院推「打詐1.5版」
  - 強化申請約定轉帳防詐
  - 納管虛擬資產交易平台業者
  - 就源處理網路假投資廣告
  - 遊戲點數防詐鎖卡及內控機制
  - 第三方支付業者建立客戶審查機制
  - 全台走透透宣導防詐

詐騙路徑及手法

詐騙集團　　中介管道　　民眾

人頭 / 車手 —開戶 (洗錢人頭帳戶)→ **銀行**

月租型人頭門號
企業門號
預付卡門號 —代收簡訊認證碼、申請免洗帳號→ **社群平台**

透過社群購買商品，付錢但拿不到貨
賣家可隨時砍帳號
受騙買家 → **社群平台**

詐騙網頁 —不實廣告上架→ **廣告平台**

民眾 —導向詐騙網頁、騙取個資/金錢→ **廣告平台**

詐騙集團 / 偽造網頁 —發送惡意簡訊→ **簡訊業者**

TA: 金融機構 → **簡訊業者**

證券客戶身分之資通防護規範

證券商客戶身分防護法遵要求

依據	規範內容	法遵重點
上市上櫃公司資通安全管控指引(111.4.7)	第五章 資通系統發展及維護安全 第13條、將資安要求納入**資通系統開發及維護需求規格，包含**機敏資料存取控制、**用戶登入身分驗證**及用戶輸入輸出之檢查過濾等。 (*See* also 第14條 定期測試、第23條 監控措施)	資安精神應落實於資通系統開發及維護。其中資安要求包含**身分驗證機制**
建立證券商資通安全檢查機制(111.12.28)	第7點 通訊與作業管理(CC-17000) d. CA認證與憑證管理 (a) 網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，**必須採用多因子（如：下單憑證、綁定裝置、OTP、生物辨識及SIM認證等）驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分**並留存紀錄。	憑證管理之多因子驗證應與客戶登入時使用之因子有別，以確保**身分驗證機制有效**
證券商受理線上開戶委託人身分認證及額度分級管理標準 (111.12.16)	證券商就線上開戶程序，應於內部控制制度自行訂定相關作業流程。**受理該類開戶作業除應確定其身分為本人及留存相關證明文件外，應先經下列第三方認證或出具本人證件以確認身分**： 一. 經往來交割銀行確認。 二. 經線上傳送自然人憑證、銀行帳戶或晶片金融卡等。 三. 經線上傳送可同時辨識國民身分證及臉部之照片，並輔以證券商交割專戶客戶分戶帳指定出金帳戶。 四. 經由視訊影像方式確認。 五. 經由行動身分識別（Mobile ID）方式確認，相關身分認證應遵循事項由本公司另訂之。 六. 透過其他可確認身分之方式 。	身分驗證機制之可信賴性，應透過**第三方認證**

ISO 29115標準之身分識別機制

階段	簡稱	主要作業內容
登錄階段 enrolment phase	登錄 enrolment	核驗並確認個體所提示的身分資料與個體之關聯性。 將完成核驗「實體世界的個體」所對應的「身分資料」進行登錄作業。
信物管理階段 credential management phases	管理 management	建立並維護個體與身分資料的關聯性。 除了管理「信物」產製、發放以及維運的整個生命週期外，尚須維護身分資料與信物之間的「連結性」及資料的「正確性」與「即時性」。
個體驗證階段 entity authentication phase	驗證 authentication	驗證個體與身分資料的關聯性。 個體提出服務相對應所需之信物，而藉由驗證信物獲得個體身分資料的過程，即為「驗證」。

信賴等級 (LoA)	說明 (對所驗證之身分的可信度)
LoA1	(Little or no) 少許或沒有可信度可言
LoA2	(Some) 具某種程度的可信度
LoA3	(High) 高可信度
LoA4	(Very high) 極高可信度

身分認證及額度分級管理標準

法規:臺灣證券交易所股份有限公司證券商受理線上開戶委託人身分認證及額度分級管理標準(111年12月16日公佈)

帳戶類型	身分認證程序	約定強度	單日買賣最高額度
第一類	一. 往來交割銀行確認。 二. 自然人憑證、銀行帳戶或晶片金融卡等資料。 三. 可同時辨識國民身分證及臉部之照片+證券商交割專戶客戶分戶帳指定出金帳戶。 四. 視訊影像方式確認。 五. 行動身分識別（Mobile ID）方式確認。 六. 其他可確認委託人方式。 **以上都需結合 OTP 或電訪。**	同意單日買賣最高額度受限。	新臺幣100萬元。
第二類	自然人憑證+視訊影像方式。	提供資力證明，如個人年所得扣繳憑單資料等。	依徵信與額度管理自律規則，由證券商自行訂定評估單日買賣最高額度。
第三類	同第一類。	約定於委託買賣時採預收或圈存方式辦理。	比照第二類辦理。

證券商行動身分識別(Mobile ID)身分認證

證券商辦理行動身分識別(Mobile ID)身分認證應循事項 (111.12.16)

第二條
行動身分識別（Mobile ID），係指證券商經取得委託人同意後，由委託人透過載有4G以上門號SIM卡之行動裝置，經第三方認證機構向委託人所屬之電信業者，以委託人之行動電話號碼、國民身分證統一編號及生日，與電信業者之行動門號租用人申辦資料進行比對，確認為一致後通知證券商，所進行之身分認證作業。

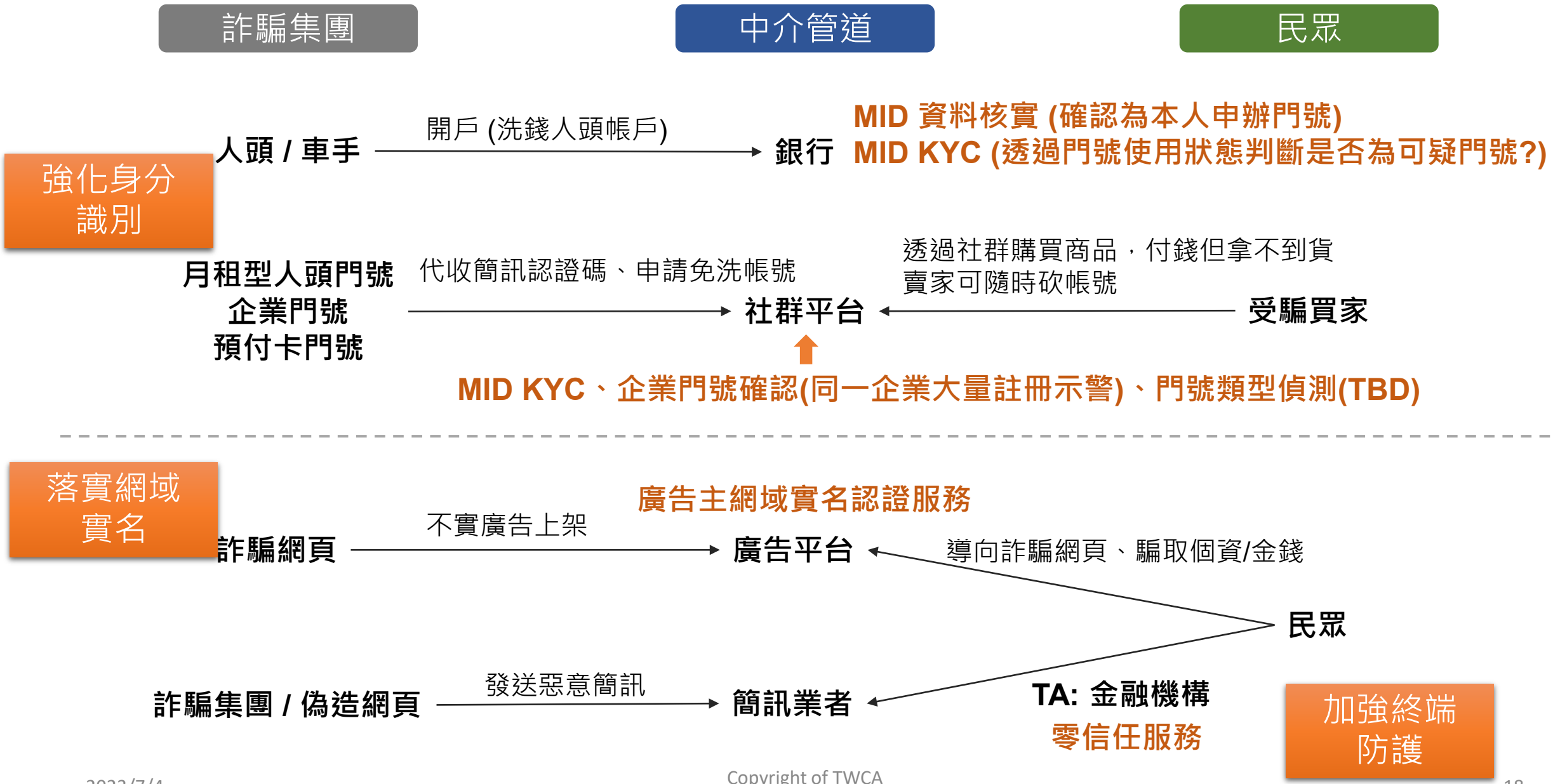
前項所稱4G以上門號，係指委託人至電信業者直營門市臨櫃申辦，交付國民身分證及具辨識力之第二身分證明文件並完成親簽後申辦之門號，且應排除儲值卡、親子卡、預付卡、企業卡、委託代辦等無法辨識本人親辦親簽之門號。

本事項所稱第三方認證機構，係指數位發展部依電子簽章法第十一條第四項規定公告核定之憑證機構。

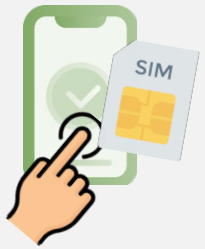
資安防護下的數位身分驗證方案

- MID KYC
- MID 企業門號確認

詐騙路徑及手法



行動身分識別 (Mobile ID)



持電信 SIM 卡客戶

TWID 身分識別中心

電信業者

門號身分識別

由電信業者比對門號申辦人留存門號、身分證字號，並確認發動交易的SIM卡與門號相符。

‘識別使用者身分’

SIM 認證

確認目前發動交易的SIM卡和要認證的門號是否相符。

‘驗證約定往來門號’

門號資料核實

由服務提供者發動查詢，門號及申辦人身分證字號是否相符。

‘核實留存資料’

MID 服務於金融產業應用現況

	門號身分識別	SIM 認證	門號資料核實
	‘識別使用者身分’	*‘驗證約定往來門號’*	*‘核實留存資料’*
銀行	**跨境支付會員帳號註冊**	**客戶設備綁定** **重新設定交易密碼** (22 家銀行)	**客戶門號定期核實**
保險	**網路會員帳號註冊** **遠距投保** **行動投保** (10 家業者)	推廣中	**保戶門號定期核實**
證券	**變更原留手機門號**	推廣中	推廣中
政府	**線上服務實名認證** (防疫、報稅、報關、勞保)	推廣中	**MyData 會員手機核實**

New

MID 企業門號確認

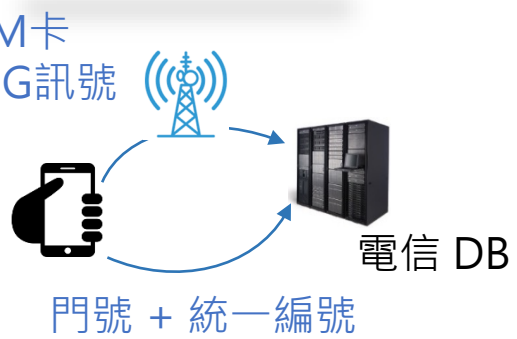
- 提供**統一編號 + 門號**作為識別因子，由電信業者判斷是否為既有的企業用戶。
- 僅能確認該門號為企業申辦，如需識別自然人，建議搭配其他檢核因子。

應用場域

身分識別機制
之**輔助因子**

驗證是否為
企業申辦之門號

企業門號確認



企業門號資料核實

發動者	用戶手機端	SP 主機端
可驗資料	1. SIM 卡 2. 門號 3. 統一編號	1. 門號 2. 統一編號
驗證限制	需使用4G/5G網路連線	無

New

MID KYC

門號樣態確認

手機(SIM卡)發動：身分證字號(ID) + 門號

TWID 身分識別中心

1. 該門號為該 ID 申辦
2. 該 ID 持有該門號是否**超過 6 個月**(門號換號或過戶..不在此限)
3. 該門號電信費帳單繳費方式是否為**自動繳款**(限金融帳戶及信用卡)
4. 該門號近6個月是否曾進入**催繳狀態**(催繳狀態僅限該門號或與該門號合併之帳單)

姓名確認

手機(SIM卡)發動：身分證字號(ID) + 門號 + 姓名(王大明)

TWID 身分識別中心

1. 該門號為該 ID 申辦
2. 該門號登記姓名是否為王大明

* 限制及資格同 MID 門號身分識別

電信使用樣態

租約期間紀錄

中華電信 Chunghwa Telecom
T STAR 台灣之星
亞太電信 Gt
台灣大哥大
遠傳 FET

MID KYC

申辦銀行業務
線上開戶、
貸放款...等

客戶同意條款

身分識別
樣態檢核

TWID
身分識別中心

客戶身分識別及電信使用樣態檢核結果

服務整合優勢

- 用戶實名認證
- 評估信賴程度
- 打擊詐欺行動

發現潛在問題點

攔阻詐騙可能性

預防人頭或車手

強化檢核因子

- 持有門號是否超過6個月
- 是否綁定金融繳款工具
- 近 6 個月是否正常繳費

資安防護下的數位身分驗證方案

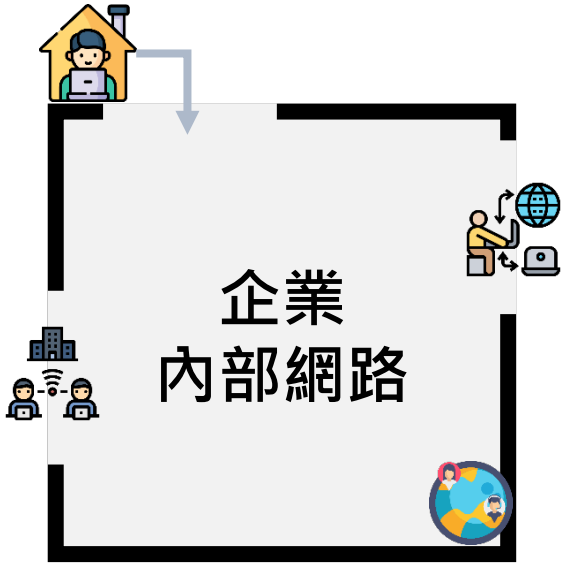
- 撞庫強化
- 零信任
- 網站實名

撞庫事件後的資安強化措施

- 第一是證券商及期貨商應使用優質密碼設定並進行管控
  - 例如：確實執行密碼輸入錯誤次數達3次，必須予中斷連線，及加強宣導客戶定期更新使用者密碼。
- 第二是證券商及期貨商應於網路下單登入時落實採多因子認證方式，
  - 例如：下單憑證、綁定裝置、OTP、生物辨識等機制，強化憑證換發的驗證機制，以確保為客戶本人登入。
- 第三是證券商及期貨商應每日針對核心系統的帳號登入失敗紀錄進行監控
  - 例如：非客戶帳號登入嘗試紀錄等，進行監控及瞭解分析異常登入原因、異常IP登入時通知投資人，並留存相關紀錄。

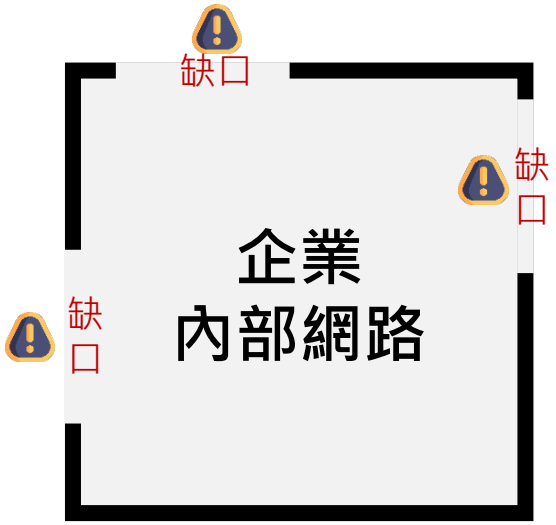
隨著時代發展，網路信任邊界模糊化

工作型態多元化



遠端工作、外包工程、
雲端服務、多元裝置...

信任邊界模糊



疫情製造了更多資安缺口

駭客入侵機會提升

時代演進，駭客能力↑

零信任是什麼?

ZTA (Zero Trust Architecture)

- 是一種資安防護的新概念，打破了傳統以邊界（例如防火牆）區分內網及外網的資安型態
- 一個關於作業流程/系統設計/營運策略的概念及指導原則

ZTN (Zero Trust Network)

- 解決現今網路環境複雜造成信任邊界不明之資安窘境，期望透過對任何資料存取皆永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證一致安全性之相關技術。
- 參考 NIST (SP 800-207)零信任架構，設計符合國內資安政策之政府零信任網路，採存取門戶部署方式，具備**身分鑑別**、**設備鑑別**及**信任推斷** 3 大核心機制

我不信任您，請您每一次進行服務登入/ 資料存取都要驗證哦！

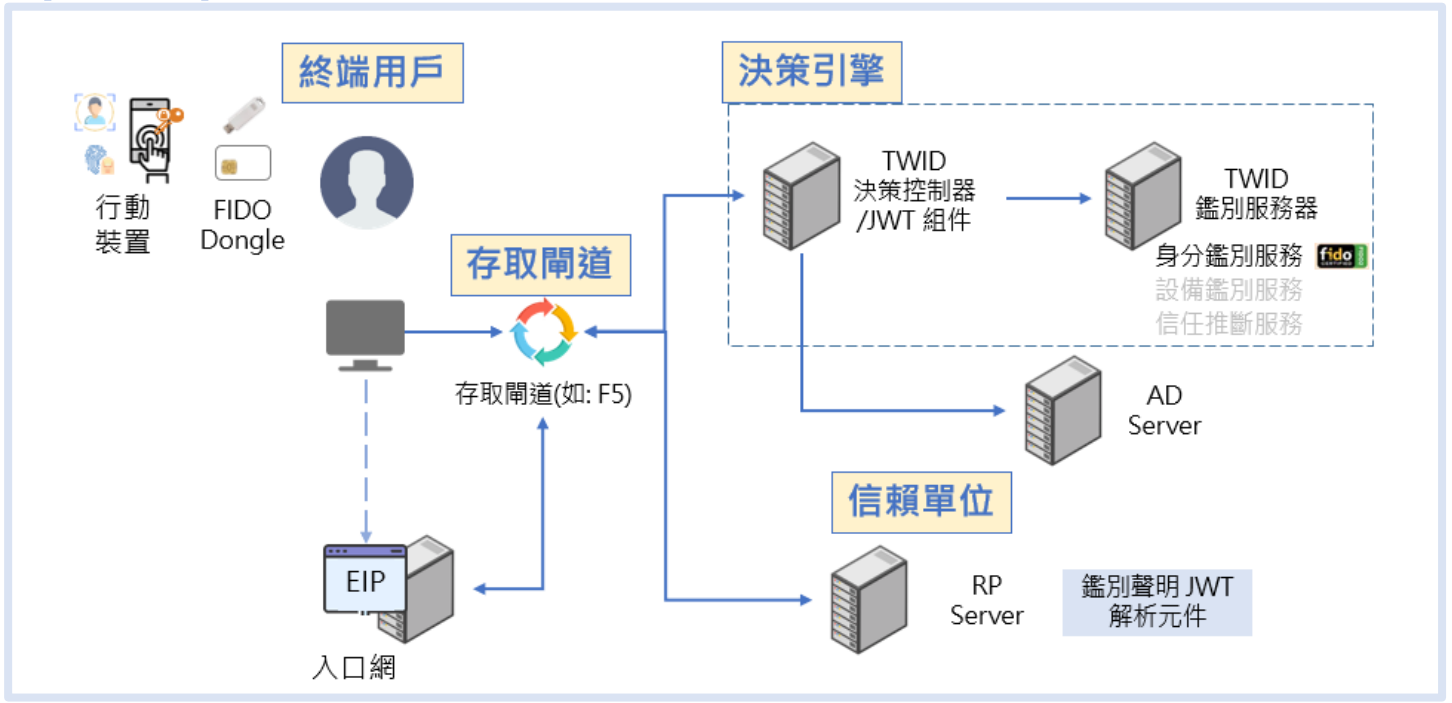
零信任網路 (ZTN) 規劃與原則

導入零信任網路**會是一段過程**，而不是一次大規模替換基礎架構，相關組件之部署須具備能與**現有系統同時混合運作**之能力。

取自：政府零信任網路說明_V1.9_1110712.pdf
https://www.nics.nat.gov.tw/ZeroTrustMain?lang=zh

建議先找單一應用場域導入

零信任網路 (ZTN) 是甚麼?



終端用戶	存取閘道(Access Gateway)	決策引擎(Decision Engine)	機關資通系統/信賴單位(RP)
欲登入 RP 人員	負責網路導向與連線，為 RP之存取門戶 • 不論來自內部或外部網路之存取，**必須且唯一**經由存取閘道 • 為唯一公開存取之組件，存取全程必須隱藏內部網路路徑(如利用**反向代理**技術) • 實施**負載平衡**機制以避免效率瓶頸 • 實施可有效防止阻斷服務攻擊之機制	**A. 決策控制器** B. 三大核心機制 **1. 身分鑑別(111)** 2. 設備鑑別(112) 3. 信任推斷(113) **C. 鑑別聲明伺服器**	• 內部系統 ✓ 公文系統 ✓ 報表系統 ✓ EIP 系統 ✓ 網管系統 ✓ 防火牆系統 • 對外服務

建議先找單一應用場域導入

零信任網路 (ZTN) 三階段規劃

	身分鑑別 (111)	設備鑑別 (112)	信任推斷 (113)
現況	• 仰賴密碼(Password)或 有風險的 MFA	• 首次設定決定未來權限 或未定義	• 首次設定決定未來權限 或未定義
政府走向	• **國際 FIDO 規範** • **私鑰存於 Client端** • **允許生物特徵結合 FIDO Key 簡便密碼輸入**	• **TPM 鑑別**設備安全性 • **動態分析**設備健康信任等級 • **控管設備**存取權限	• 透過**身分鑑別、設備鑑別**及**匯整各類輸入資料**(如:使用者IP) 推估信任分數

零信任網路 (ZTN) 第一階段說明

身分鑑別 (111)

傳統
(現在)

- 仰賴密碼(Passwor
或 有風險的 MFA

政府
走向

- **國際 FIDO 規範**
- **私鑰存於 Client端**
- **允許生物特徵結合 FIDO Key 簡便密碼輸入**

您的指紋有誤！
請重新辨識！

Fast IDentity Online (FIDO)

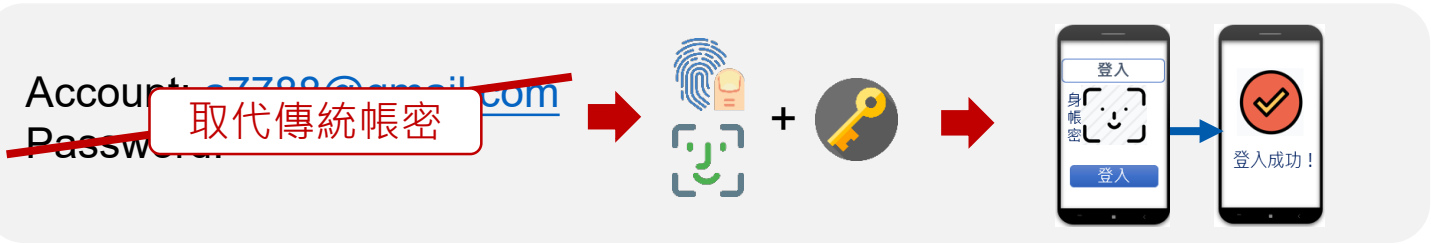
結合**公開金鑰、生物特徵**等技術，提供便利且安全的網路**身分驗證機制**，並依此建立產業標準。

無密碼 解決傳統密碼及 OTP 的安全性不足等問題

國際標準 FIDO 身分識別國際標準

行動化 人手一機，導入快速/體驗最好

安全性 非對稱金鑰之簽驗章技術為基礎



零信任網路 (ZTN) 第一階段說明

身分鑑別 (111)

傳統
(現在)

- 仰賴密碼(Passwor
  或 有風險的 MFA

政府
走向

- **國際 FIDO 規範**
- **私鑰存於 Client端**
- **允許生物特徵結合 FIDO Key 簡便密碼輸入**

您的指紋有誤！
請重新辨識！

臺網 FIDO ID 特色

FIDO Key 結合 憑證 應用更多元

- **系統登入 (身分識別)**
- **強化機制 (多因子機制)**
- **服務申辦 / 主管放行**
- **文件簽署 (不可否認性)**

零信任網路 (ZTN) 第二階段說明

設備鑑別 (112)

傳統
(現在)

- 首次設定決定未來權限
未定義

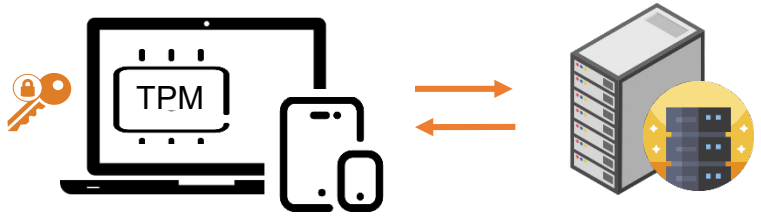
政府
走向

- **TPM 鑑別**設備安全性
- **動態分析**設備健康信任
- **控管設備**存取權限

每次針對設備行安全性檢查
例如設備太舊，可能會顯示
無法滿足資料取用資格！

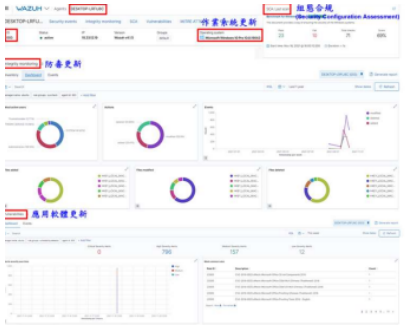
設備 TPM 鑑別

– 執行基於TPM內私鑰之公開金鑰密碼系統鑑別協議



設備健康管理

– 持續更新設備健康狀態
– 依設備健康狀態隨時換算設備健康信任等級



設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

健康狀態/等級分配
(A)作業系統更新：0.4
(B)防毒更新　　：0.3
(C)應用軟體更新：0.2
(D)組態合規　　：0.1

零信任網路 (ZTN) 第三階段說明

信任推斷 (113)

傳統
(現在)

- 首次設定決定未來權限
  未定義

政府
走向

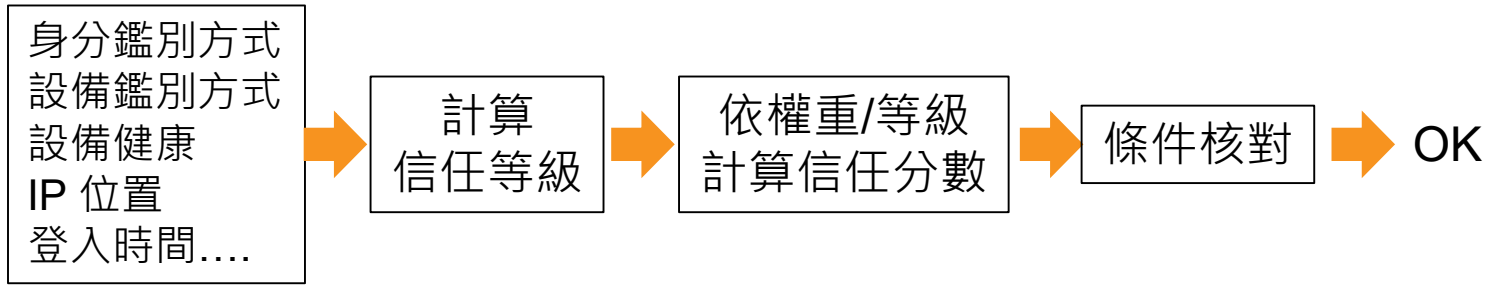
- 透過**身分鑑別、設備鑑**
  匯整各類輸入資料(如
  者IP) 推估信任分數

如果信任推斷的資訊顯示
安全，可能會限制權限或
求重新登入！

信任推斷機制

建置信任推斷前端系統，匯整各類輸入資料，透過信任推斷伺服器，進行(智慧)評估與計算，輸出信任分數

- 輸入：身分鑑別方式、設備鑑別方式、設備健康信任等級、及使用者情境(IP位址、登入時間、瀏覽器等)
- 輸出：信任分數，供決策控制器做存取決策



網站實名制

網站擁有SSL憑證並無法保障網站安全。網路釣魚詐騙中，詐騙集團慣以免費、自動化、開放憑證架設釣魚網站，透過平台投放不實廣告；或利用簡訊夾帶惡意連結，混淆一般消費者或投資者誤信，致個人資料遭洩漏或財產等損失。而企業型憑證或稱延伸驗證憑證（EV SSL/TLS）為具有最高層級加密、驗證和信任之數位憑證。申請EV SSL/TLS時，企業或網站擁有者必須接受憑證機構嚴格審查，審查範圍例如實體公司、使用網域專屬權利等。以驗證等級而言，憑證可區分為以下三類：

項目	基本型（DV）	進階型（OV）	企業型（EV）
驗證等級	域名驗證 (Domain Validation, DV)	組織驗證 (Organization Validation, OV)	延伸驗證 (Extension Validation, EV)
驗證方式	網頁驗證檔、DNS、E-mail	人工驗證	
驗證對象	域名持有人	域名持有人、公司證明文件	域名持有人、公司證明文件、第三方驗證
適用範圍	個人網站	一般商業機構	金融機構、資安防護需求企業
憑證特性	發證快速	憑證登載組織資訊	憑證登載組織資訊、網址列標示組織名稱

敬請指教

臺灣網路認證公司

TWCA 臺灣網路認證

TWID 身分識別中心