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

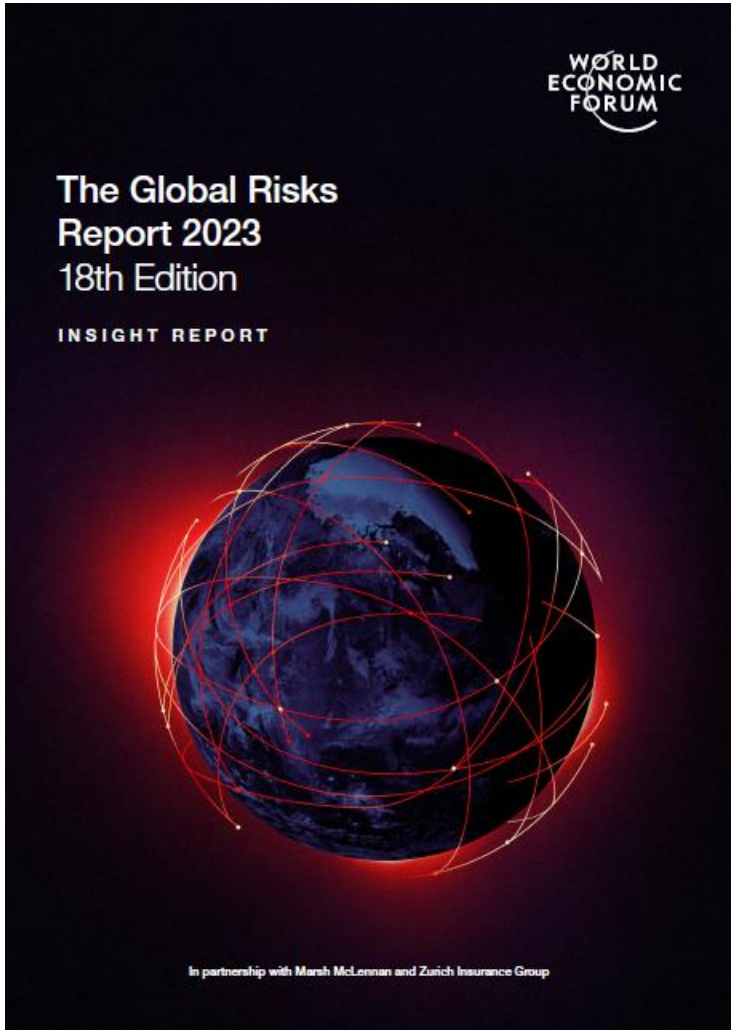
全球風險趨勢

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。**

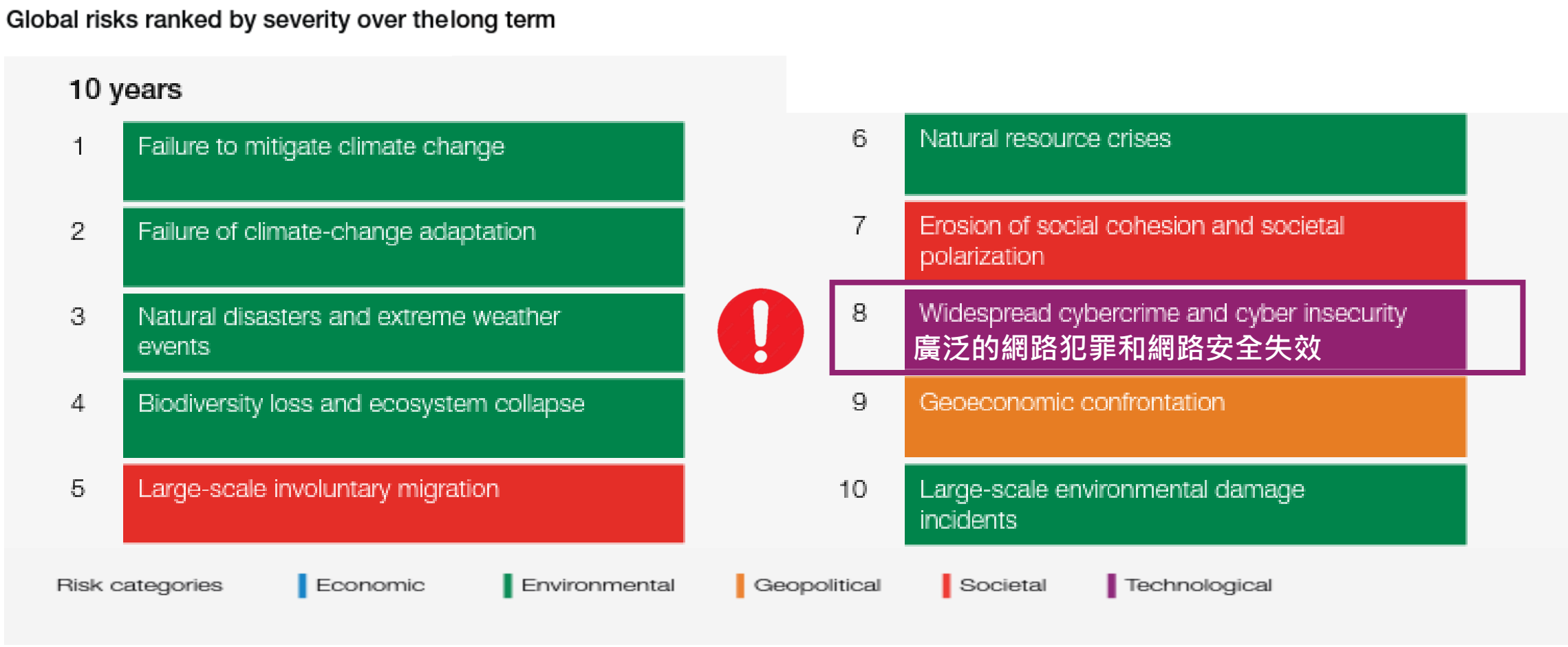
針對國家**關鍵基礎設施的網絡攻擊**已被列為2023 年全球性風險前五名。



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。

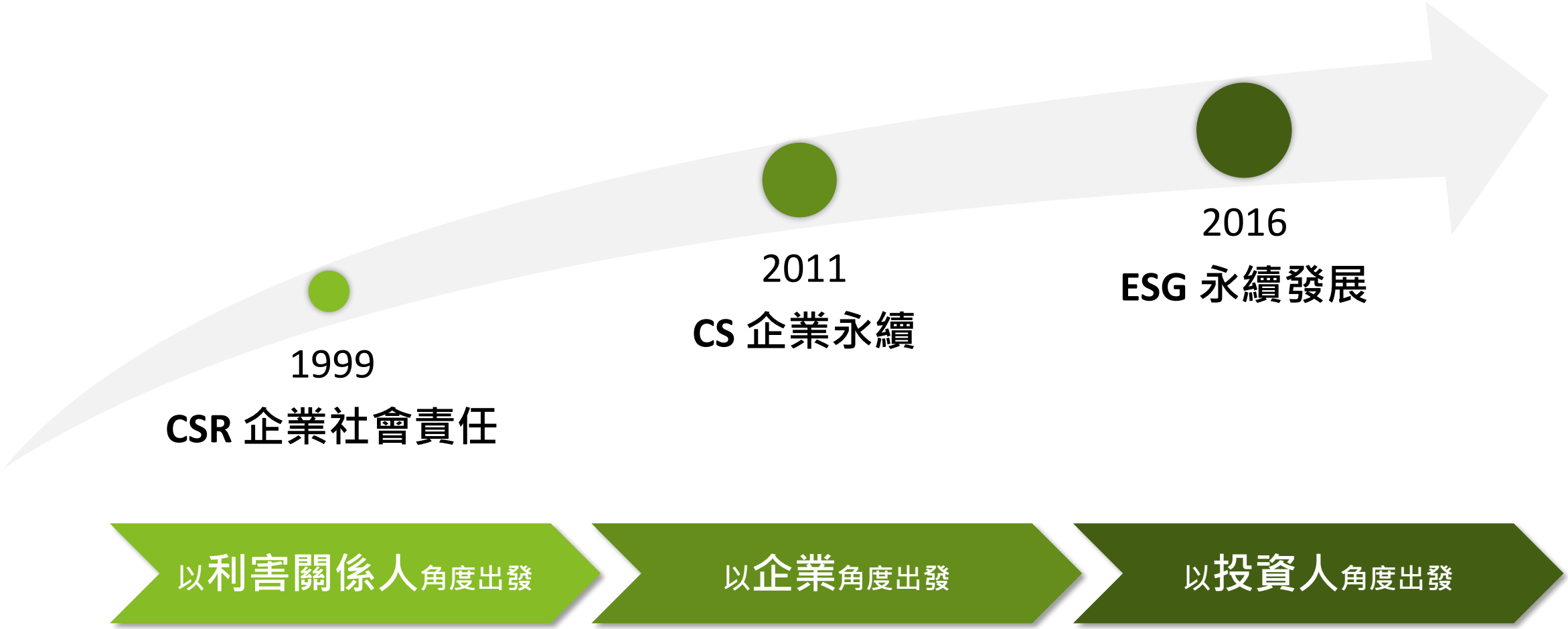
根據世界經濟論壇2023年報告指出，「廣泛的網路犯罪和網路安全失效」是未來十年風險排名前10名的新成員。



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。

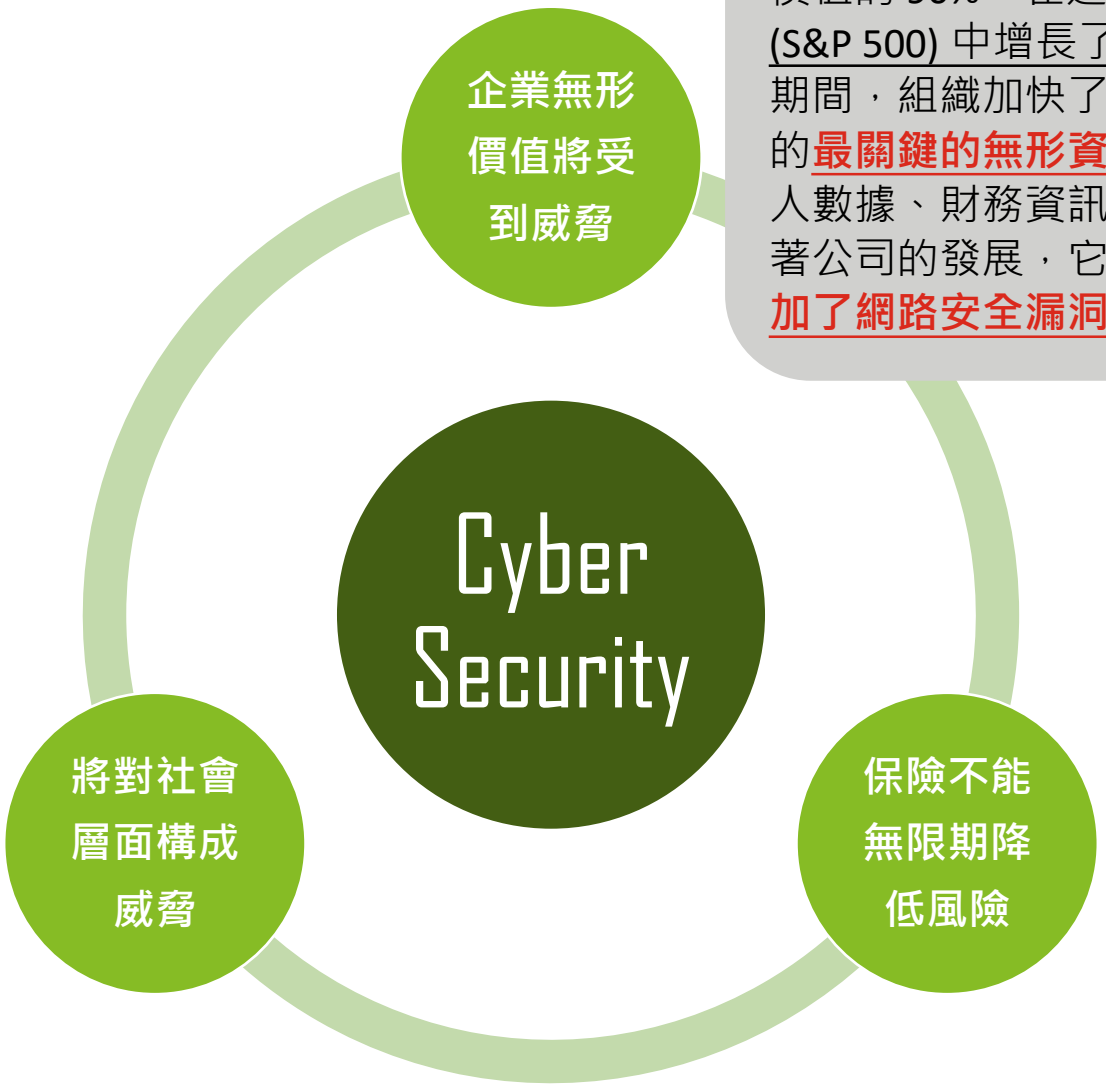
法遵風險

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。**

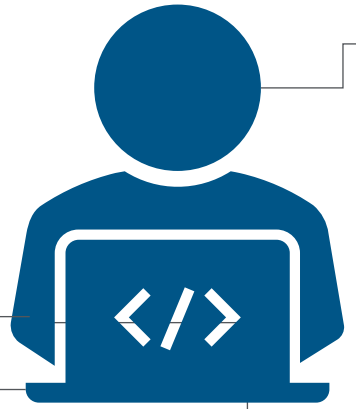
臺灣金融相關產業重大資安事件

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。

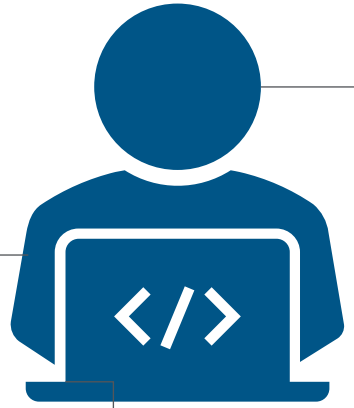
(2022.12)因內部優化系統影響效能，導致用戶登入網銀緩慢，引爆民怨。

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。



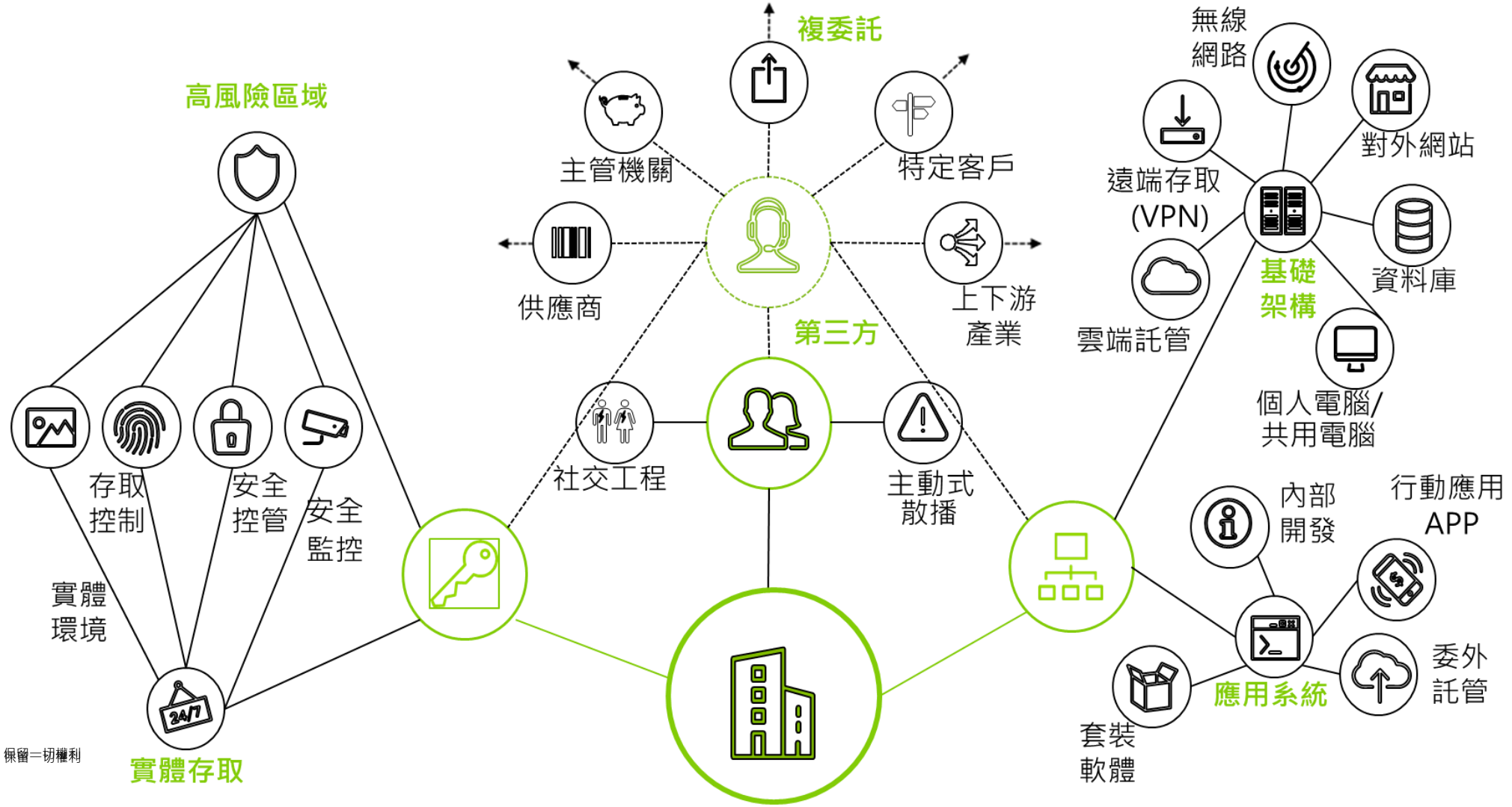
BSI銀行(Bank Syariah Indonesia)
(2022.05)印尼的BSI銀行受到網路攻擊並且被知名勒索軟體組織LockBit竊取1,500萬名客戶或員工之個人資訊(如姓名、手機號碼、地址、帳戶餘額等)，除了ATM 與移動銀行 (m-banking) 服務中斷、遭威脅勒索高達2,000萬美金的贖金外，最終導致1.5TB機敏資訊被公開。

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...

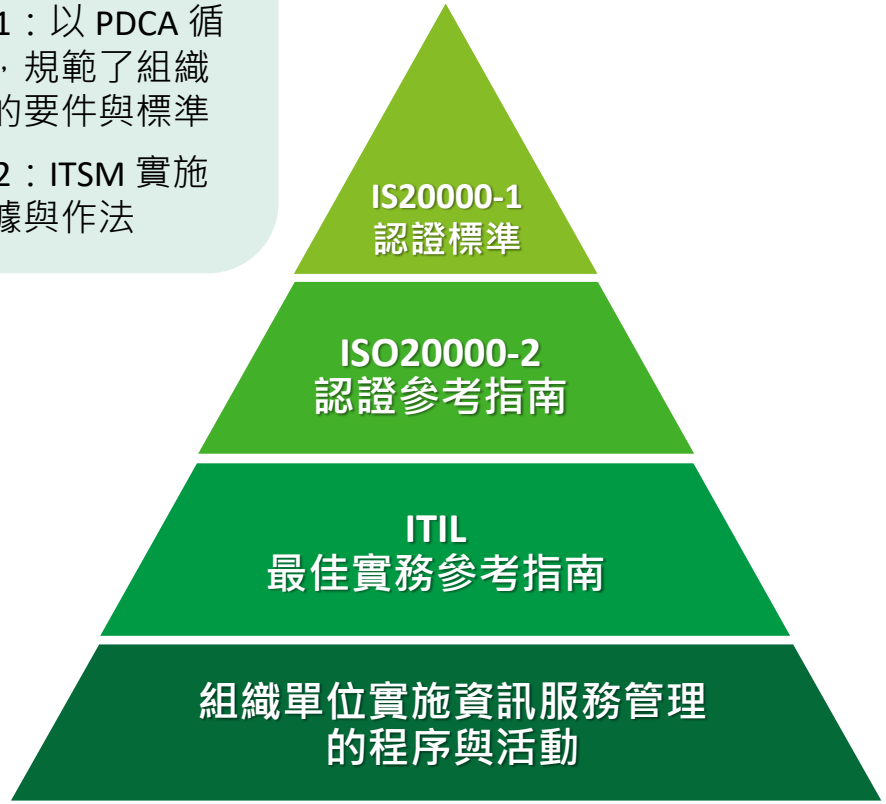
確認組織相關的利害關係人，了解其期望，共享資訊、知識與資源；外部提供者管理...

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)

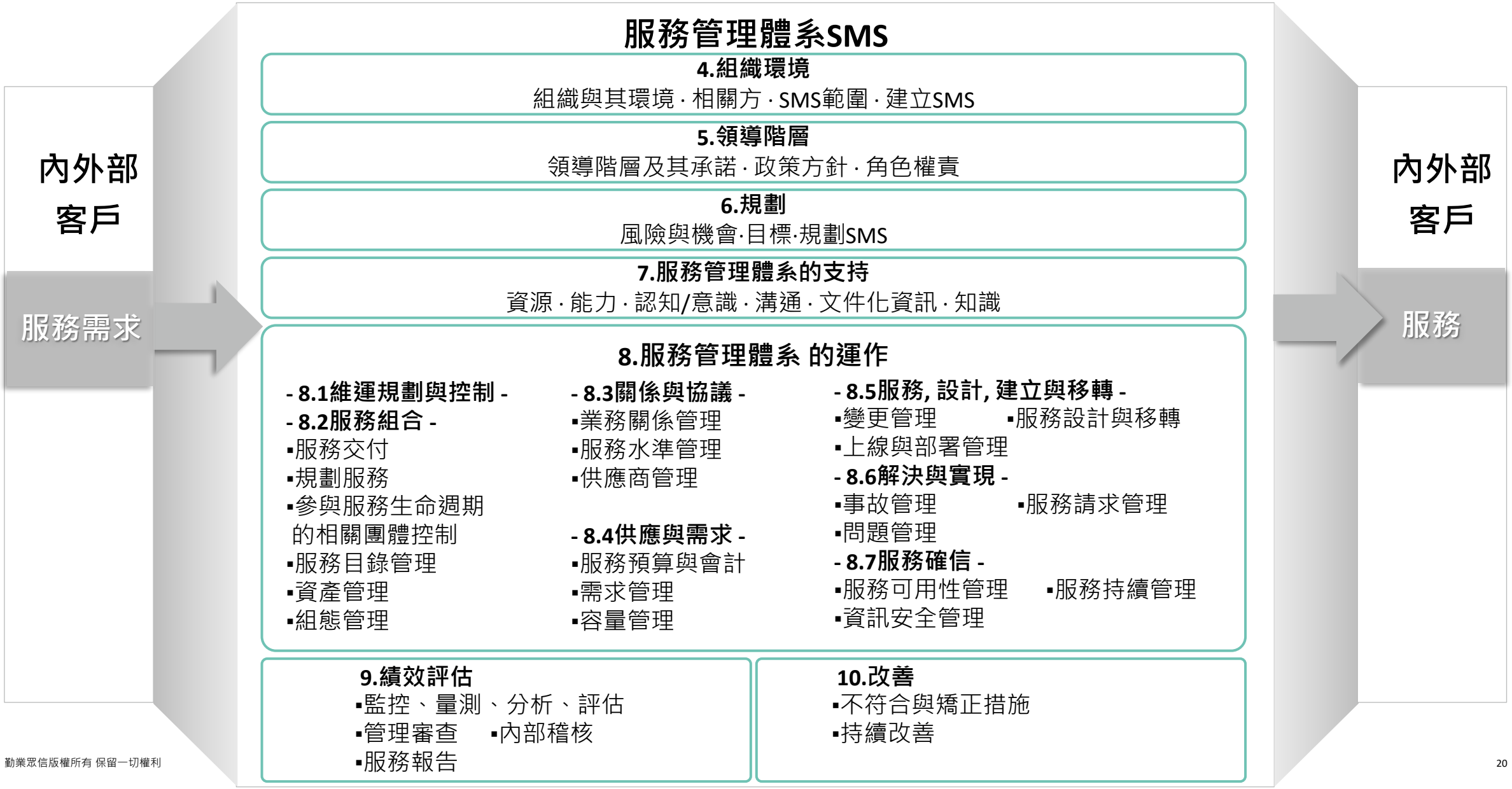
4.服務異常處理與後續問題診斷

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

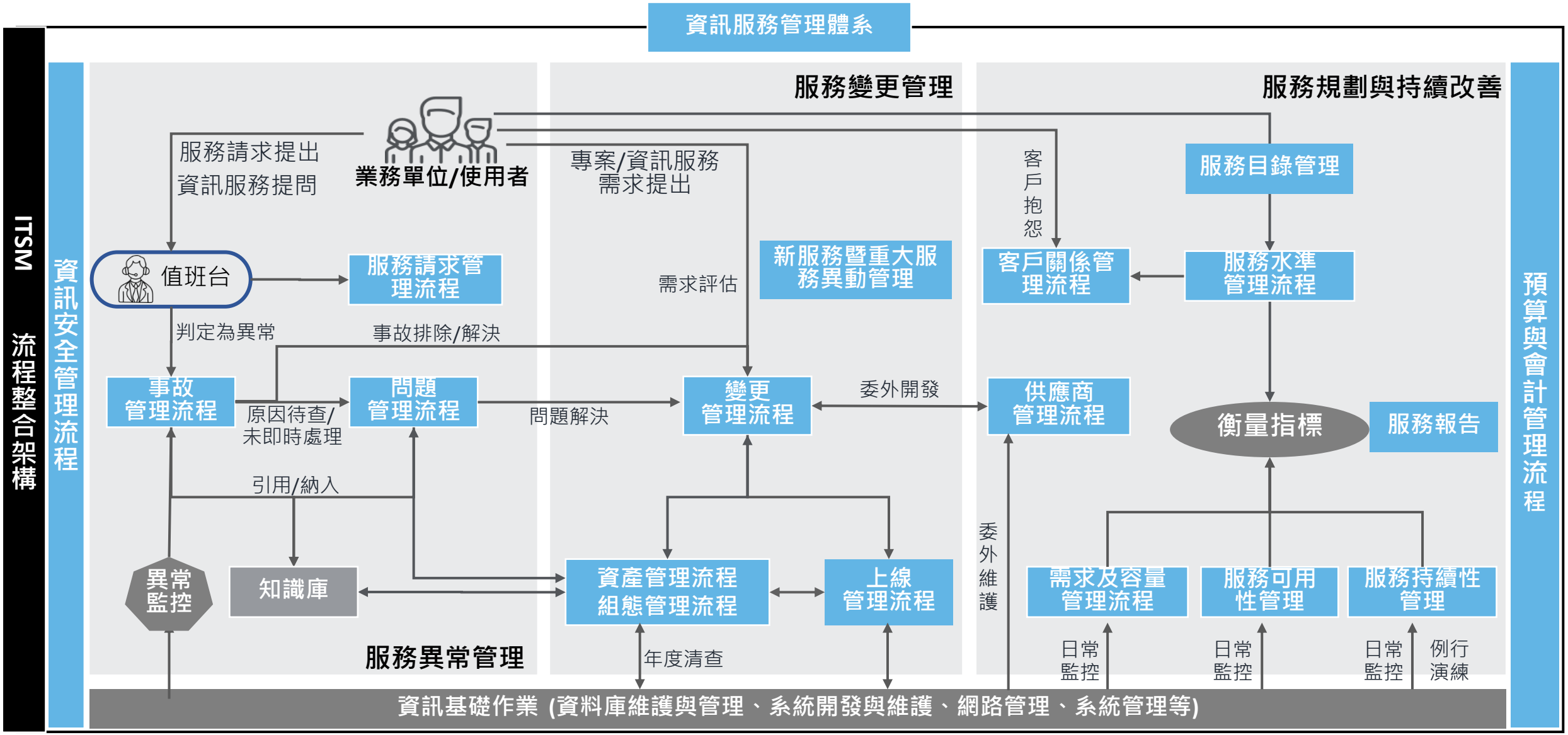
5. IT 服務持續改善

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



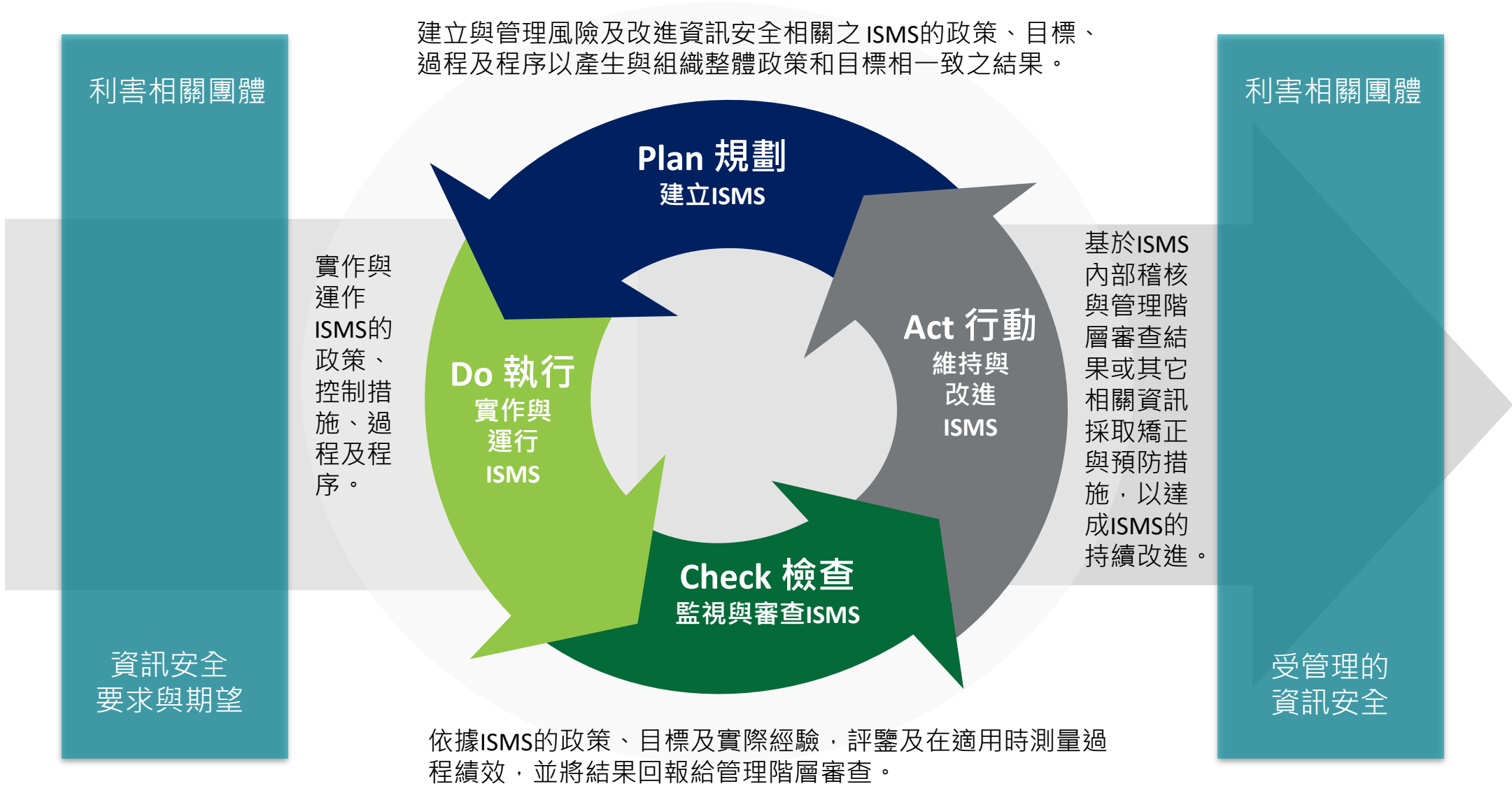
資訊服務管理各流程關聯



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

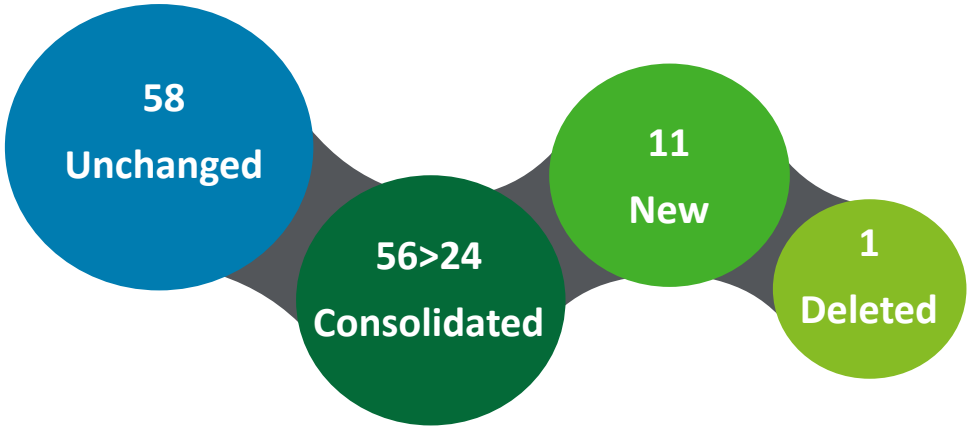
Ch1. 適用範圍(Scope)
Ch2. 引用標準(Normative references)
Ch3. 名詞與定義(Terms and definitions)
CH4. 組織背景(Context of Organization)
Ch5. 領導力(Leadership)
Ch6. 規劃(Planning)
Ch7. 支持(Support)
Ch8. 運作(Operation)
Ch9. 績效評估(Performance evaluation)
Ch10.改善(Improvement)

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

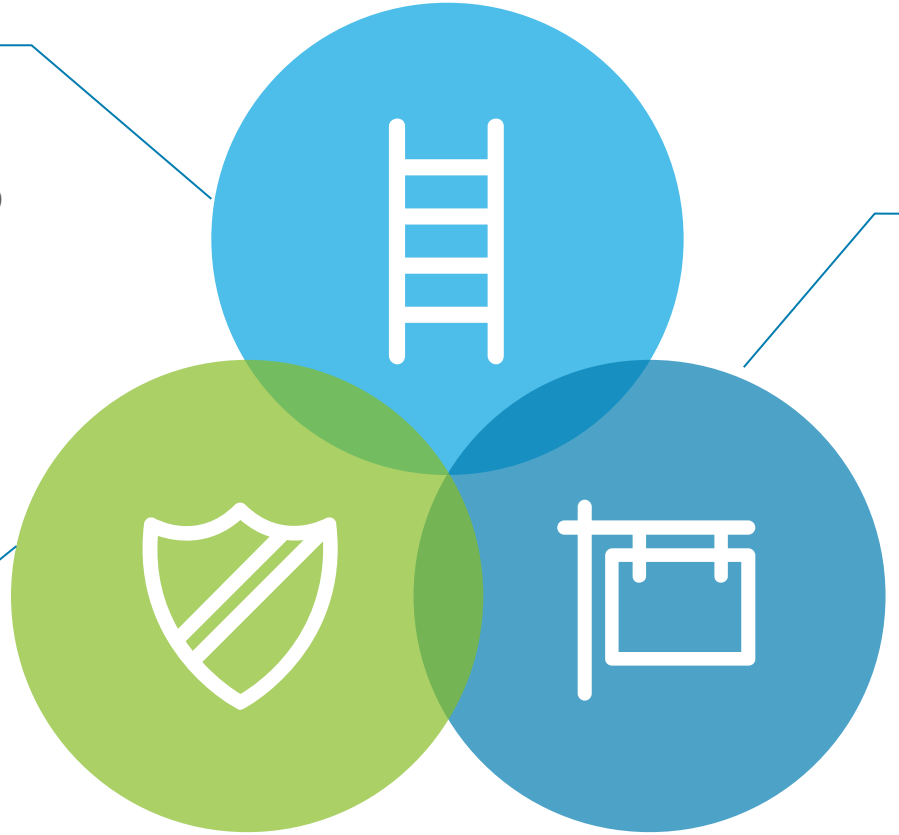
通過對於隱私保護的控制實現對ISMS進行補充，使企業建立PIMS，實現有效的隱私管理，從而使企業獲益。

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

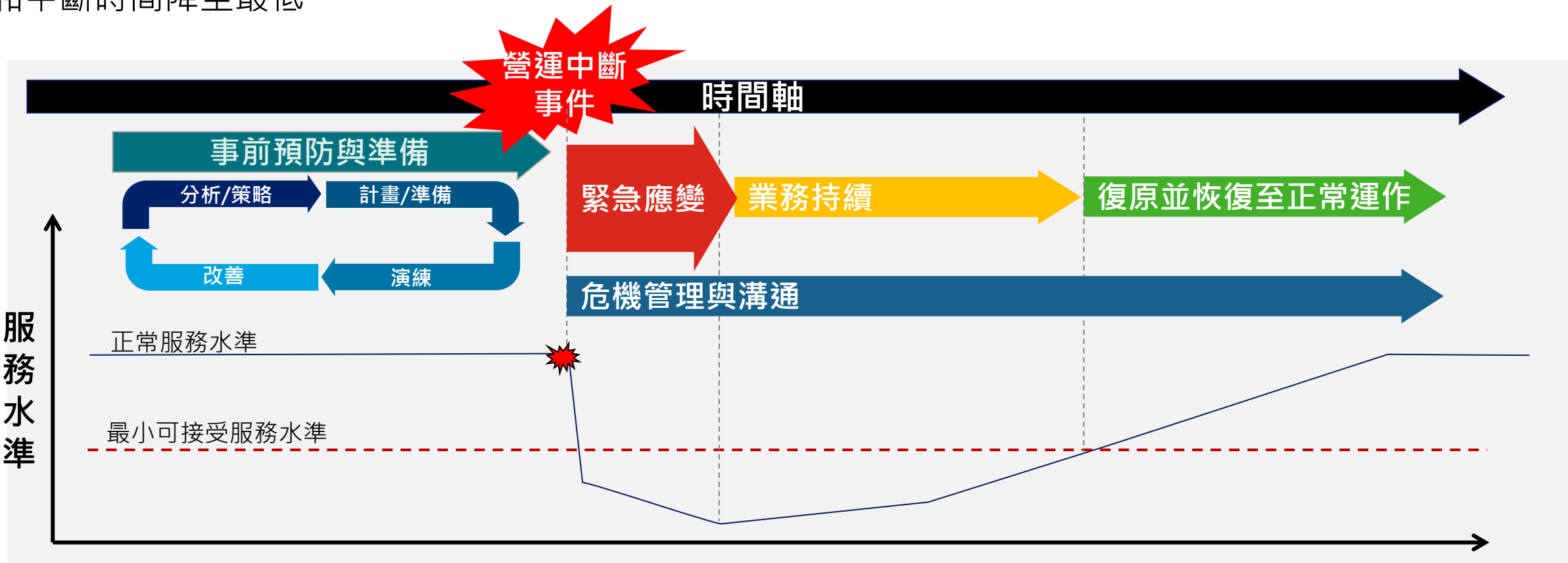
- PII: Personally Identifiable Information 個人可識別資訊

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

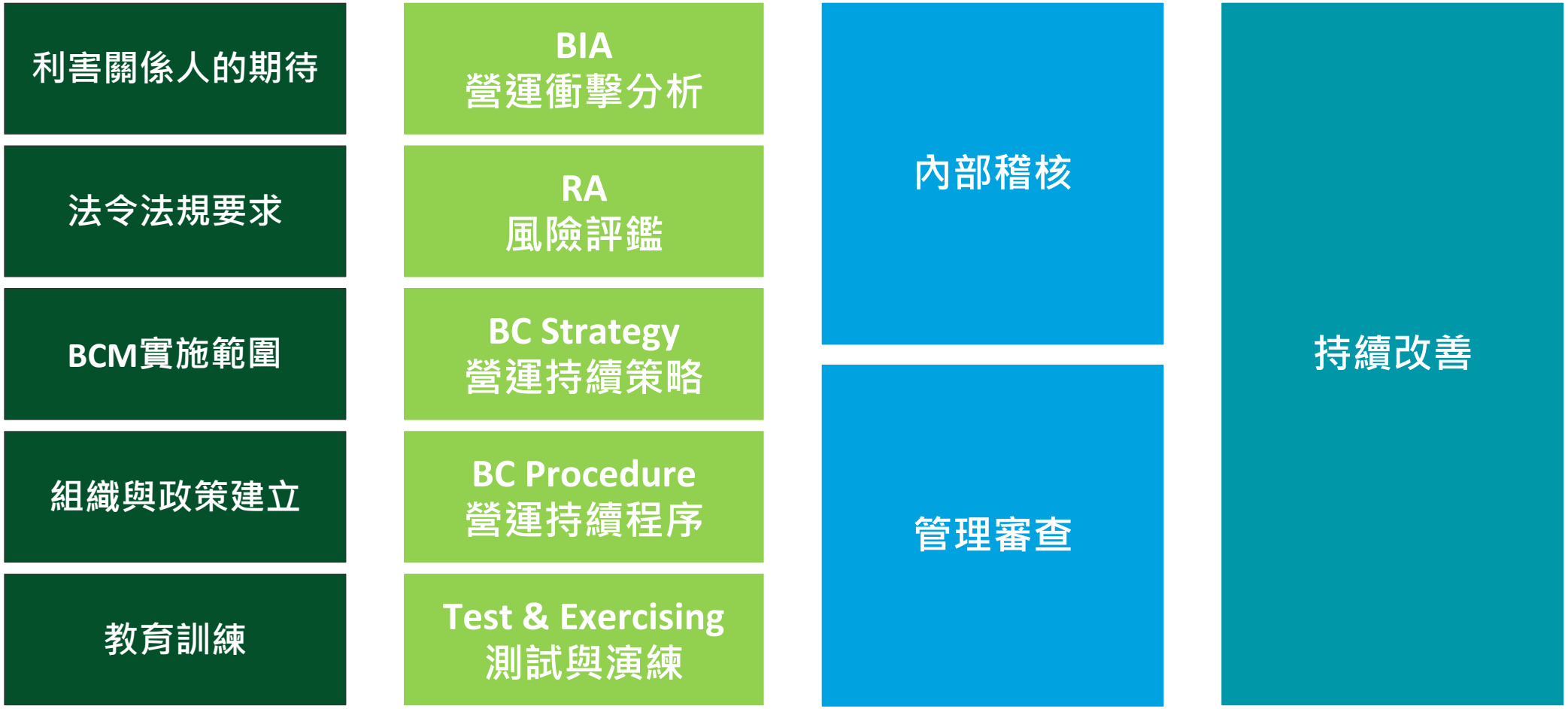
資訊系統故障

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