資訊安全與個資保護介紹

講師:李雋元
Email:ericph0617@gmail.com

課程大綱

- 近年來網站側錄以及個資外洩案例
- 資訊保護與個人隱私重要性
- 資訊安全管理系統說明
- 個資保護管理制度介紹

世界經濟論壇的《2019年全球風險報告》

- 包含電腦犯罪與網路攻擊、資料詐欺或竊盜、關鍵資訊基礎設施破壞與科技發展造成負面影響被認為是2019年的可能影響風險

英航38萬客戶個資被駭 遭判罰近3億美元

- 英國航空公司(British Airways)的母公司國際航空集團(IAG)今天(8日)表示，英航因為去年遭駭客入侵，駭客只在該網站所使用的Modernizr程式庫裡，埋入了22行程式碼，就得手了38萬名旅客的個資與付款資訊，被判處1億8,339萬英鎊(大約2億2,970萬美元)的罰款 。
- 國際航空集團發表聲明說，英國資訊專員辦公室(Information Commissioner's Office, ICO)根據英國的資料保護法(UK Data Protection Act)，要對英航祭出這筆罰款單。這項罰款相當於英航2017年營業額的1.5%。
- 國際航空集團執行長華爾希(Willie Walsh)表示，他們正打算採取所有適當措施，以強力捍衛英航的立場，因此，他們考慮上訴，英航董事長兼執行長克魯茲(Alex Cruz)則對這項罰款感到意外和失望。
- 歐盟的個資保護法(GDPR)在去年5月25日生效，被稱為是史上最嚴格個資保護法；然而，去年9月，英航就傳出遭駭客入侵，遭竊走38萬名客戶的個資，包括姓名、郵件地址、電子郵件信箱以及信用卡資訊等。

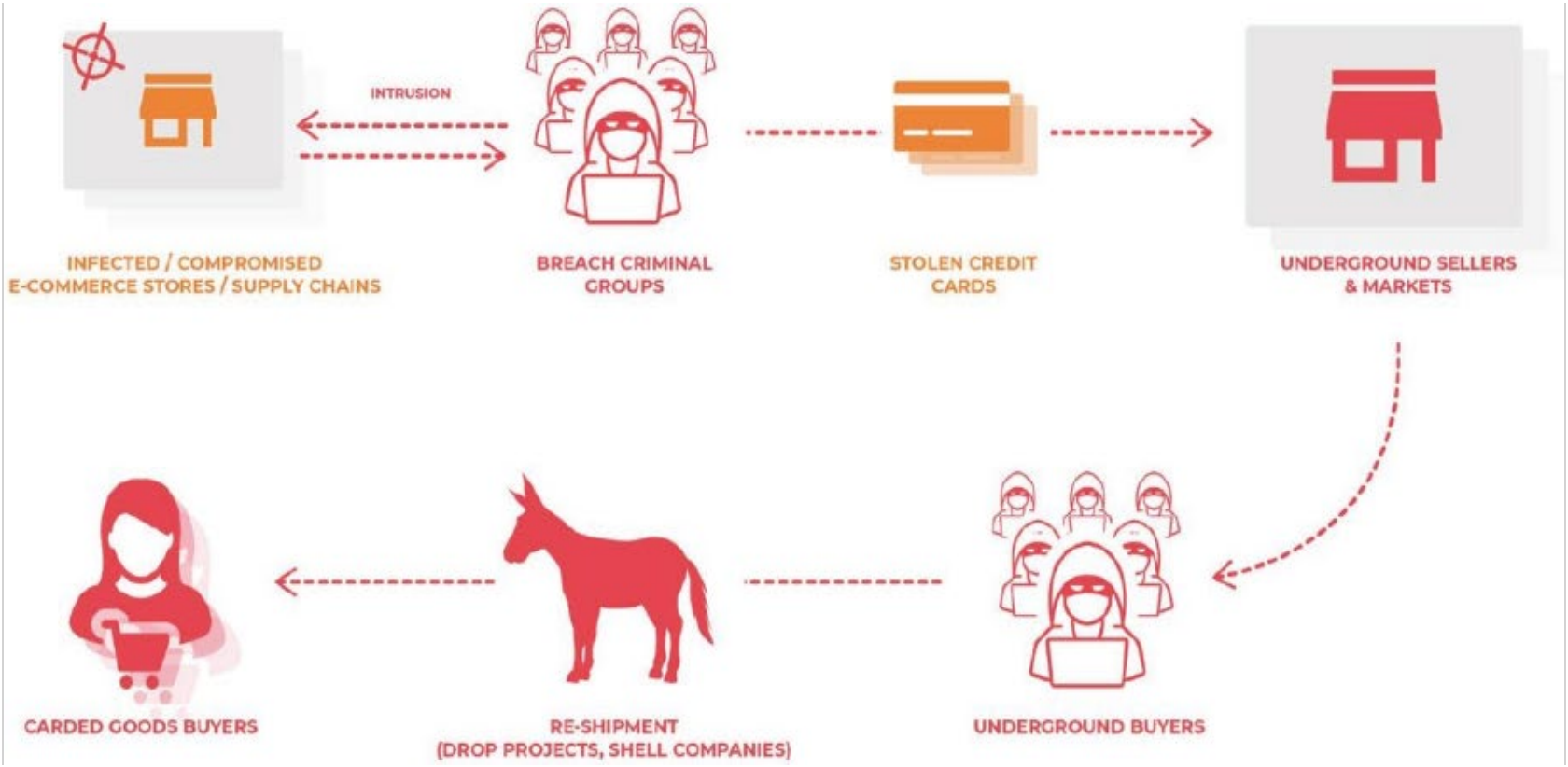
Ticketmaster使用的第三方通訊軟體遭駭，客戶資料外洩

- 根據Ticketmaster在6月27日公布的資訊，他們於同月23日，在英國版網站上，發現第三方廠商Inbenta的提供客戶支援通訊程式裡，含有惡意軟體。隨後，該公司便停用旗下所有網站上的同款通訊軟體。
- 駭客利用指令碼滲透的方式，在電子商務網站上，側錄使用者輸入線上交易表單的內容。
- 該公司網站原編寫的內容，已幾乎被駭客改寫，並非單純只有針對Ticketmaster。因此，他們認為，同樣使用Inbenta軟體平臺的線上交易系統，其中所含的用戶交易資訊，也可能面臨遭側錄的風險。

網路罪犯透過表單點擊劫持快速致富

- 表單點擊劫持攻擊操作簡單又能帶來獲利：網路罪犯將惡意程式碼置入零售商的網站中，竊取消費者的信用卡詳細資料，平均每個月有 4,800 多個獨立網站遭受入侵。
- 知名企業 (Ticketmaster 和 British Airways) 與中小型企業均遭受攻擊，去年保守估計為不肖份子帶來數千萬美元的獲利。
- 每張信用卡在地下交易論壇最高可售得 45 美元，因此只要在每個受入侵的網站竊取 10 張信用卡，即可帶來每月高達 220萬美元的獲利。單單 British Airways 攻擊事件就有超過 38萬張信用卡遭竊，歹徒所得淨利可能超過 1,700 萬美元。

網站側錄與漏洞問題更加嚴重



（圖片來源／RiskIQ、Flashpoint）

59萬筆「八大情治個資」外洩!!網路賤賣350元

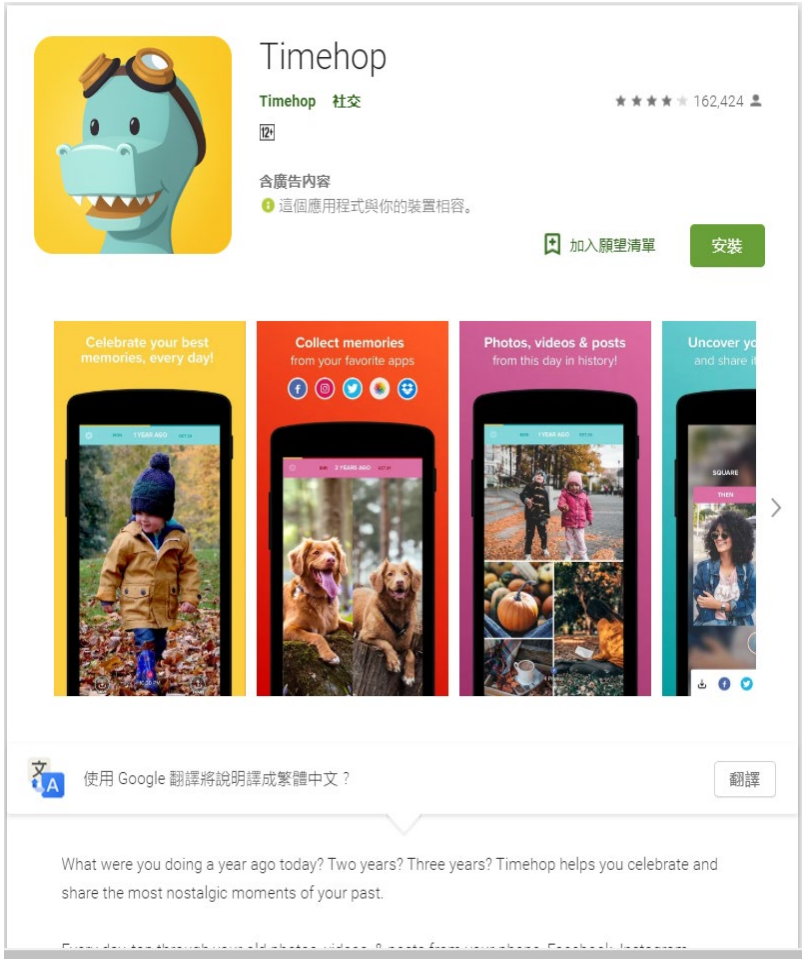
- 英等國組成的情報交換網「5眼聯盟」日前輾轉通知台灣這起重大資安事件後，經行政院緊急調查，發現包括國安局、軍情局、調查局、警政署、檢察、海巡、政風及憲兵等8大情治系統個資全都流出。6月22日，行政院高層收到由美國、英國、加拿大、澳洲及紐西蘭等國組成的五眼聯盟（Five Eyes）提供的情資，發現銓敘部高達59萬筆公務員個資遭外洩，事件震動府院高層。
- 行政院國家資通安全會報立即開會因應，除了通報相關單位應變之外，也全面清查外洩管道及遭洩露的個資範圍。
- 根據資安官員清查結果，目前已鎖定外洩個資來自銓敘部的一部電腦主機，經資料比對，發現2004年即被植入木馬程式，目前遭洩露的個資經查是2012年6月初流出，由於該系統在2015年3月就已下線更新，卻還難以避免資料遭外洩，相關單位不排除是維修人員、內鬼或駭客所為，已啟動調查程序，防止事件擴大。
- 原文網址: https://www.ettoday.net/news/20190703/1480994.htm

個資外洩發生的產業

- 2019/2發布「2019 4iQ Identity Breach Report」報告。報告中指出，2018年總計有12,449起新的身分外洩事件，比2017年增加424%。
- 若從外洩事件發生的產業別來看，論壇以27.5%位居第一，居次的是政府機關12.2%，遊戲產業占11.8%，電子商務網站占11.7%，教育/學術界則占9.2%。
- 2018年最大宗的個人身分資料外洩事件為澳洲安全專家Troy Hunt在駭客論壇上所發現的Collection #1，包含逾11億組的電子郵件+密碼，以及超過7.7億個不重覆的電子郵件帳號。
- 值得注意的是，這些在網路上流竄的個人身分資訊只有37%是因為遭到駭客攻擊而外洩，卻有63%是因為意外才曝光。

Timehop驚爆遭駭，2100萬個資外洩

- 2018年7月4日提供臉書及推特過去貼文回顧的app
- Timehop周日公告上周7月4日遭駭傳出重大資安事件，2100萬名用戶個資外洩，而且駭客也曾取得用戶存取臉書、推特、IG等社交網站內容的憑證。



個資外洩醜聞，Facebook 遭英國開罰

- 2018 年 3 月劍橋分析公司（Cambridge Analytica）被爆出非法從 Facebook 獲取超過 5 千萬人的個資，後來 Facebook 將受害人數上修到 8,700 萬。Facebook 早在 2015 年就得知劍橋分析公司違規，卻未公布這項訊息，反而將相關的資料銷毀。
- 英國資訊專員辦公室在 7 月 10 日宣布，由於 Facebook 沒有妥善的保護用戶的資料將裁罰 50 萬英鎊，約相當於台幣 2,000 萬元
- 歐盟已經生效的一般資 料保護規定(General Data Protection Regulation, GDPR)，針對資訊洩漏對個人、企業及政府所造成的影 響與日俱增
- 號稱「史上最嚴格個資法」的歐盟《一般資料保護規範》(General Data Protection Regulation, GDPR) 在 2018年 5月上路了

個資外洩集體訴訟

- 美國加州舊金山一份法庭文件顯示，因一宗觸犯隱私權之集體訴訟，Google 已同意支付 U.S.$ 8,500,000.的合解金。7位原告指控 Google 免費電子郵件服務之 Gmail 內建的 Buzz 社交網路工具，侵犯其隱私權。
- Google 於 2010 年 2 月 9 日推出將 Gmail 連絡人自動掛到 Buzz 之連絡人名單中的新功能，引發網友疑慮；目前 Google 已改變其組態，Gmail 用戶必須在 Buzz 工具下，另建可以公開的連絡人名單，隨時可以瀏覽、編輯、隱藏或封鎖。
- 和解金中 30%歸律師，7 位原先每人至多可獲得 U.S.$ 2,500.，其餘金額將存入專戶，資助致力於網路隱私或教育之相關機構。
- 資料來源：http://zh.wikipedia.org/zh-tw/Google_Buzz/ (2010-09-11)。

iOS App未經同意暗中側錄用戶資訊

- Techcruch最新一次調查蒐集了多家知名公司，包括訂房及訂票網站、流行服務品牌、電信、航空公司及銀行、金融業者的iOS App。結果發現所有廠商，包括Holister、Expedia及加拿大航空等知名企業的，都沒有在服務條款中提及會紀錄使用者App的螢幕畫面，自然也就沒有取得用戶同意這回事，用戶當然也對這些行為一無所知。
- 此外，Abercrombie & Fitch、Hotels.com和新加坡航空還使用一家用戶使用經驗分析平台Glassbox的服務，在其App中嵌入連線重播（session replay）的技術。該技術可錄下用戶使用App時的每個點擊、按鍵與鍵盤輸入的內容動作，然後回傳給App開發商，有的則是回傳給Glassbox的雲端平台作為用戶行為分析。
- 但是和Techcrunch合作的安全研究公司，利用中間人攻擊工具（man-in-the-middle）從中攔截這些App回傳時的流量時，發現部份公司如加拿大航空的App，並沒有實作完整的資料遮罩，以致於用戶信用卡號碼、生日與住址可被明碼取得。

課程大綱

- 近年來網站側錄以及個資外洩案例
- 資訊保護與個人隱私重要性
- 資訊安全管理系統說明
- 個資保護管理制度介紹

現實世界 v.s. 虛擬資訊世界

現實世界	資訊世界
可以做實體身分確認	缺乏強健身分確認
了解嚇阻犯罪活動是必要的風險及成本	不了解嚇阻犯罪活動是必要的風險及成本
犯罪的方法有限	犯罪方法一直在變化
入侵或偷竊很容易被發現	破壞及犯法行為很容易不被發現
安全課題是固定,並以產品為主	安全課題是變動,並且以流程為主
犯罪預防技術可以相等或弱於犯罪技術	犯罪預防技術必須遠高於犯罪技術

安全性之基礎-資訊的定義

- *Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.*
- “資訊可以許多形式存在。可以書寫或列印於紙上，儲存在電子儲存媒體上，以郵寄或電子儲存媒體傳輸，顯示於影片上或在對話中說出。
- *Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.’*
- 不管資訊的形式是什麼，或者共用或儲存的方式是什麼，都應該受到適當的保護。

資訊安全(Information Security)的目標

- 資訊安全(Information Security) 保護資訊之機密性、完整性與可用性；得增加諸如鑑別性、可歸責性、不可否認性與可靠性。
  - 機密性(Confidentiality) 資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
  - 完整性(Integrity)對資產之精確與完整安全保證的特性。
    - (i)可歸責性(Accountability) 確保實體之行為可唯一追溯到該實體的特性。
    - (ii)鑑別性(Authenticity) 確保一主體或資源之識別就是其所聲明者的特性。鑑別性適用於如使用者、程序、系統與資訊等實體。
    - (iii)不可否認性(Non-repudiation) 對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。
  - 可用性(Availability)已授權實體在需要時可存取與使用之特性。
  - 可靠性(Reliability)始終如一預期之行為與結果的特性。

個人隱私及社會安全的危害

- 網際網路具有快速及大量傳播的能力，當個人資料輕易洩漏或竊取
  - 例： 個人身分資料 、信用卡 、銀行交易往來紀錄 外洩等
- 越依賴網路之便利性則「水能載舟 、亦能覆舟」
  - 例 電腦病毒的危害 敏感資料的竄改等

隱私權與個人資料保護

- 『隱私權』和『個人資料保護』，常常被當成一件事來談，因為『個人資料』保護不周，就可能會發生『隱私權』侵害的問題。儘管如此，還是得釐清這兩者在根本意義的異同。那就是：
  - **隱私權**，個人人格上的利益不受不法僭用或侵害，個人與大眾無合法關聯的私事，亦不得妄予發布公開，而其私人活動，不得以可能做成一般人的精神痛苦或感覺羞辱之方式非法侵入的權利。是個人的基本權利之一，受到憲法所保障
  - **個人資料保護**；則是著重於如何確保個人資料之蒐集，處理與利用過程不會侵害到『隱私權』
  - **個人資料檔案**；指基於特定目的儲存於電磁紀錄物或其他類似媒體之個人資料之集合。

隱私權保護範圍

- 司法院大法官於釋字第585號解釋，明白承認隱私權受憲法所保障，隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。
- 依釋字603號解釋，至於隱私權的保護範圍，可分為「空間隱私」與「私密隱私」兩部分。
  - 所謂私密隱私，指「保障個人生活私密領域免於他人侵擾及個人資料之自主控制」，
  - 所謂空間隱私，指「保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」

隱私權(Privacy)與資訊安全

- 隱私權 (Privacy)
  - 指個人能控制其“私人資料”的權利,避免被揭露或未經個人同意而被使用
- 新的資安趨勢中，大部分意圖竊取機密與個人資料資料；其中可側錄用戶端上網能力的威脅占了76%
  - 該功能可用以竊取如網路銀行帳戶憑證等資料，組織嚴密的地下經濟，專門販售遭竊的機密資訊，特別是信用卡與銀行帳戶憑證。

個人資料保護之國際發展

1890年隱私權的提倡
個人可不被打擾，安靜獨處生活的權利（the right to be alone)

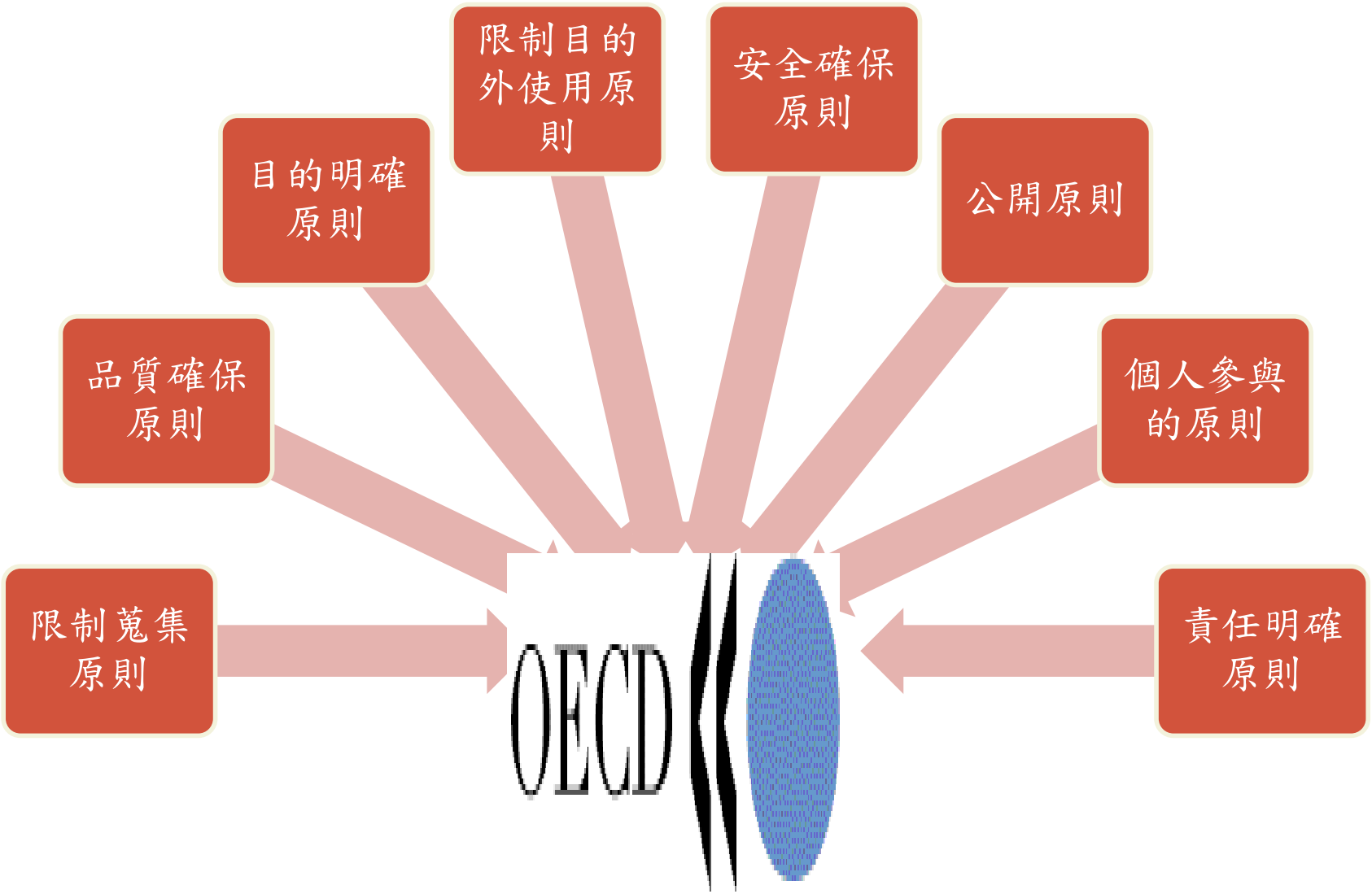
1980年隱私與個資保護開始受到國際組織重視
OECD提出「隱私保護與個人資料跨境流通指導原則」

1995年歐盟提出個人資料保護指令
歐盟個人資料保護指令，影響包含我國在內之各國立法工作

2007年APEC推動跨境隱私保護實驗計畫
我國為APEC成員之一，直接面臨來自國際上的壓力

國內個人資料保護法進度

OECD指導原則


限制目的外使用原則
安全確保原則
目的明確原則
公開原則
品質確保原則
個人參與的原則
限制蒐集原則
責任明確原則
OECD

歐盟提出個人資料保護指令

- 歐盟對網際網路應用以及電子商務環境所引發之個人隱私權利保護相當重視並有立法與規範制定的機制。1980年歐洲議會完成了有關保護個人資料之「保護自動化處理個人資料公約」
- 並已於1985年10月1日正式生效，現今已有許多歐洲國家加入，為目前世界第一個有拘束力之關於隱私權保護的國際公約。

各國落實個人資料保護採取之策略—歐洲(1/2)

- 《**一般資料保護規範**》（英語：General Data Protection Regulation，縮寫作 GDPR；歐盟法規編號：(EU) 2016/679），是在歐盟法律中對所有歐盟個人關於資料保護和隱私的規範，涉及了歐洲境外的個人資料出口。GDPR 主要目標為取回公民以及住民對於個人資料的控制，以及為了國際商務而簡化在歐盟內的統一規範。
- GDPR取代了歐盟在1995年推出的歐盟個人資料《資料保護指令》（Data Protection Directive）95/46/EC，該條例包含有關處理歐盟內部資料主體的個人可識別資訊的條款和要求，適用於與歐洲做生意的所有企業，無論位置如何。
- 處理個人資料的業務流程必須在設計和默認情況下構建資料保護，這意味著個人資料必須使用假名(pseudonmisation)或完全匿名(data anonymisation)進行存儲，並且默認使用盡可能最高的隱私設置，以避免公開資料未經明確同意，並且不能用於識別沒有單獨存儲附加訊息的主題。任何個人資料除非在法規規定的合法基礎上完成，否則資料控制者或處理者已經從資料所有者那裡獲得明確的選擇同意。資料所有者有權隨時撤銷此權限。

各國落實個人資料保護採取之策略—歐洲(2/2)

- 個人資料處理者必須清楚地披露任何資料收集，聲明資料處理的合法基礎和目的，保留資料的時間以及是否與任何第三方或歐盟以外的國家共享資料。
- 用戶有權以通用格式請求處理器收集的資料的便攜式副本，並有權在特定情況下刪除其資料。 公共主管部門和以核心活動為中心定期或系統地處理個人資料的企業需要雇用資料保護官員（DPO）負責管理GDPR的合規性。如果資料洩露對用戶隱私產生不利影響，企業必須在72小時內報告任何資料洩露。
- 本法案在2016年4月27日通過，兩年的緩衝期後，在2018年5月25日強制執行[4]。根據歐洲聯盟運作條約第288條第2項，因為GDPR屬於歐盟條例（英語：regulation；德語：Verorderung），不是指令（英語：directive；德語：Richtlinie），所以不需經過歐盟成員國立法轉換成各國法律，而可直接適用。隨著英國在2019年脫離歐盟，它於2018年5月23日御准批准了2018年資料保護法案（Data Protection Act 2018），該法案包含了相應的法規和保護措施。

各國落實個人資料保護採取之策略—美國(1/2)

- 不同於歐盟重視以立法方式保護個人資料，美國向來強調業者自律，聯邦層級至今並無一部統一適用之個人資料保護法制，而是散見於各個不同部門之立法
  - ¯醫療及保險業紀錄：「健康保險流通與責任法案」
  - （Health Insurance Portability and Accountability Act ）
  - ¯電話通聯記錄：「電子通訊隱私權法」
  - （Electronic Communications Privacy Act）
  - ¯有線電視用戶消費記錄：「有線通訊政策法」
  - （Cable Communications Policy Act）
  - ¯其他
- 為成為歐盟指令所稱之具「適當」資料保護法制之國家，2000年7月，美國與歐盟達成「安全港架構協議」（**Safe Harbor Framework**），並於同年11月生效¯參與本協議之美國業者可在美國商務部的監督管理之下，傳輸歐盟會員國國民的個人資料

各國落實個人資料保護採取之策略—美國(2/2)

- 安全港架構協議七大原則規範
  - 通知
  - 選擇
  - 同時傳遞
  - 安全
  - 資料之真實性
  - 存取
  - 執行

APEC推動跨境隱私保護

- 2004年10月通過「APEC隱私保護綱領」(APEC Privacy Framework)，針對APEC各會員體，推動整合性的個人資料保護措施
  - 2007年1月通過「跨境隱私保護規則」(Cross Border Privacy Rules, CBPR)，制定業者於跨國傳輸個人資料時所須遵循之規則
  - 2007年6月起，針對前述的跨境隱私保護問題，推動「開路者倡議實驗計畫」(Pathfinder)
  - 我國自1991年起成為APEC會員體，直接面對來自APEC及其他會員體的壓力

APEC推動跨境隱私保護

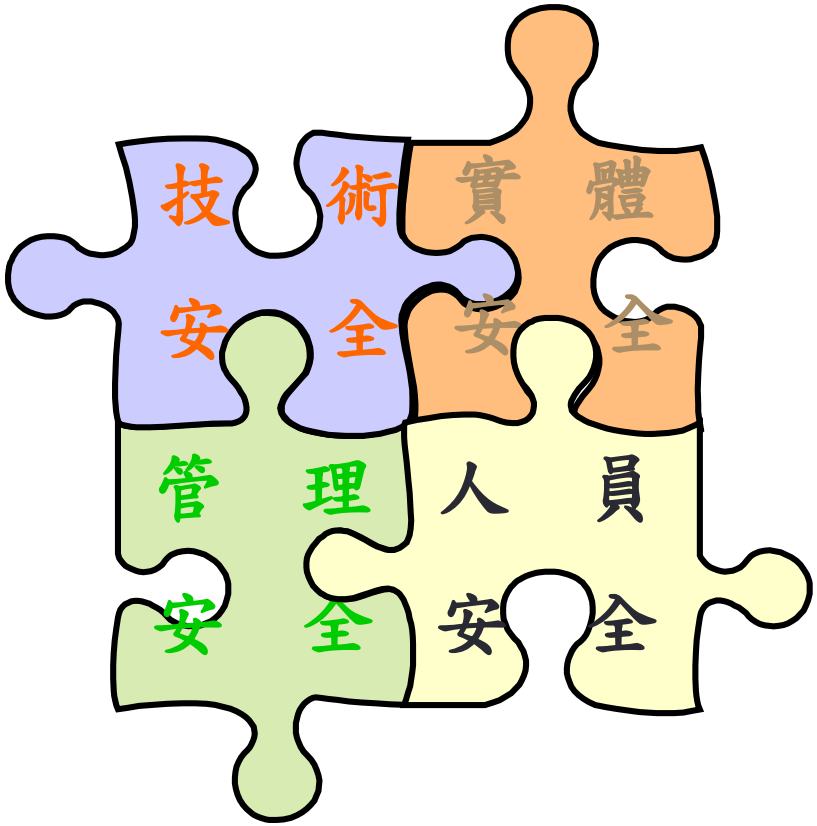
- **APEC跨境隱私保護開路者倡議計畫**
  - 1、建立企業自我評量準則
  - 2、建立信賴標章組織參與跨境隱私保護規則之準則
  - 3、檢視各組織遵守跨境隱私保護規則之狀況
  - 4、盧列協助進行跨境交易糾紛處理組織之名單
  - 5、盧列各經濟體掌管跨境資料隱私保護之官方單位及負責人名單
  - 6、建立界定跨境組織間合作之合約或備忘錄範本
  - 7、建立處理跨境交易糾紛之表單範本
  - 8、建立各經濟體主管單位執行跨境隱私保護之指導原則及程序
  - 9、發展執行跨境隱私保護準則及行動綱領之前導個案。

課程大綱

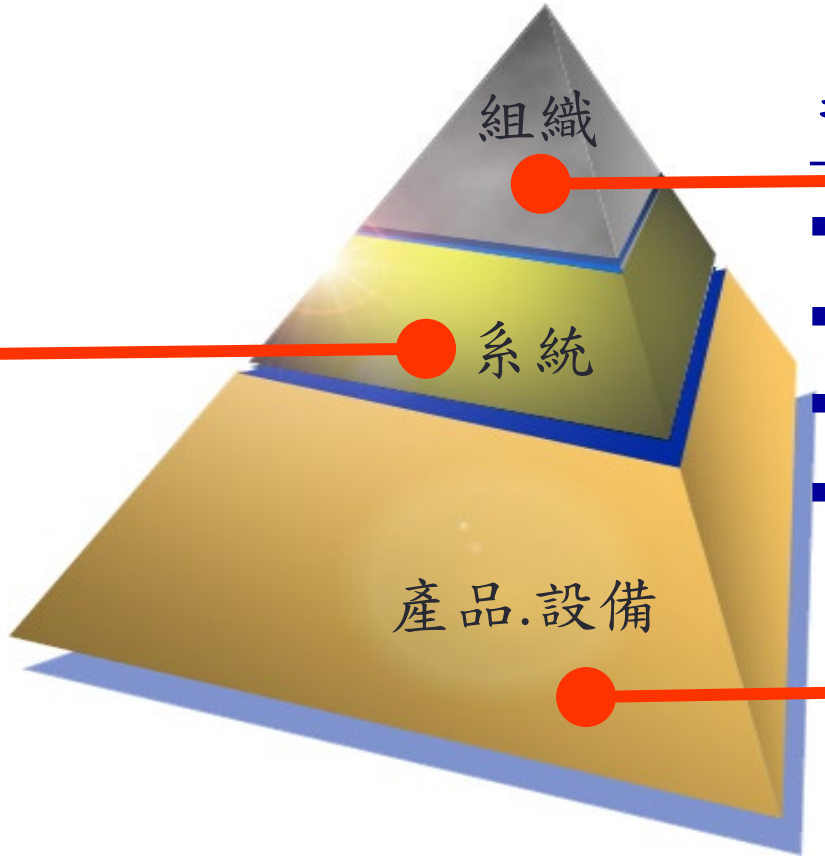
- 近年來網站側錄以及個資外洩案例
- 資訊保護與個人隱私重要性
- 資訊安全管理系統說明
- 個資保護管理制度介紹

安全管理

- 管理控制(administrative controls)
  - 政策、標準、指導原則、作業程序……
- 技術、作業控制(technical controls)
  - 身分驗證、存取控制、密碼學……
- 實體控制(physical controls)
  - 環境控制、門禁管制、設備維護……
- 人員安全(Personal Security)



完整的資安防護體系



資安管理制度

- ISO27000系列
- COBIT
- ITIL，ISO20000
- GDPR

系統安全

- 作業系統
- 網　路
- 應用系統
- 實體安全

安全產品

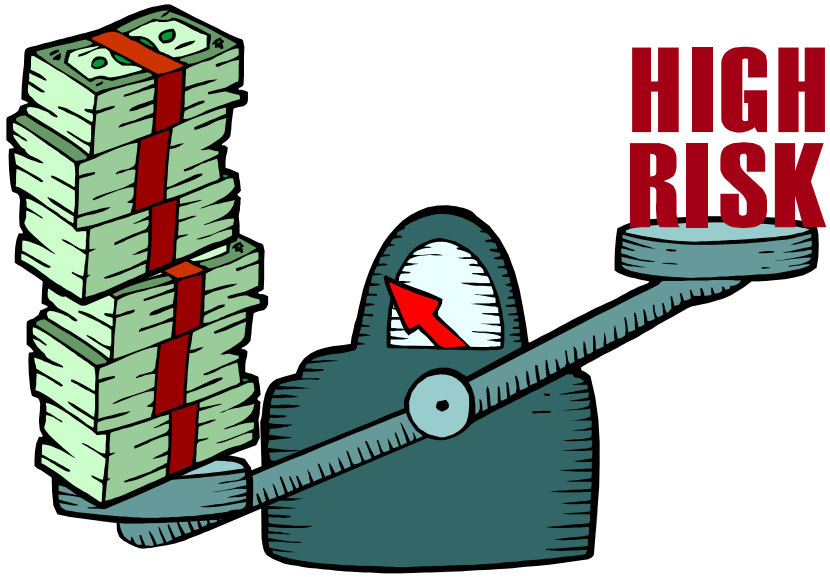
- 軟體 AntiVirus
- 硬體 IPS、Virus Wall

資訊安全(Information Security)

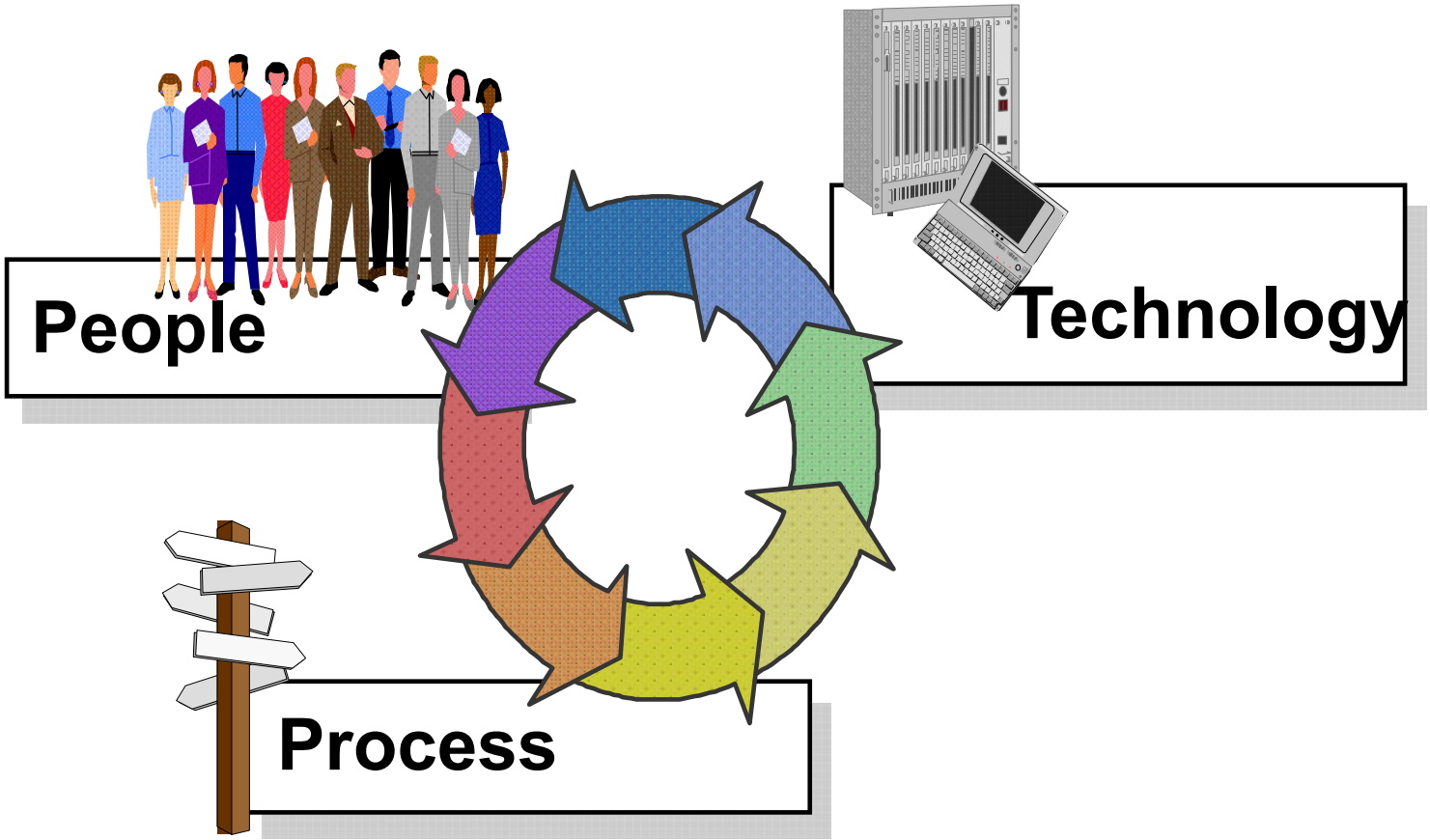
- 資訊安全 (Information security) 是指資訊的保密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability) 的維護。不同類型的資訊及其相對應資產的資訊安全在機密性、完整性、及可用性方面關注點不同。
- 資訊、支援作業、系統及網路都是重要的營運資產，資訊的機密性、完整性及可用性，攸關能否維持競爭力、現金流量、獲利能力及商業形象。但很多資訊系統在設計時就不夠安全，透過技術手段達到的安全性亦有限，所以必須透過適切的管理及程序支援。
- 為了識別有哪些控制措施需要縝密的計畫並注意細節，資訊安全管理的最低要求是組織內所有員工的參與以及供應商、客戶或股東的參與，亦可能需要外部專家的建議。在要求規格和設計階段就加入資訊安全控制措施，將更有效率，從長遠來看亦具成本效益。

資訊安全管理系統 (Information Security Management System)

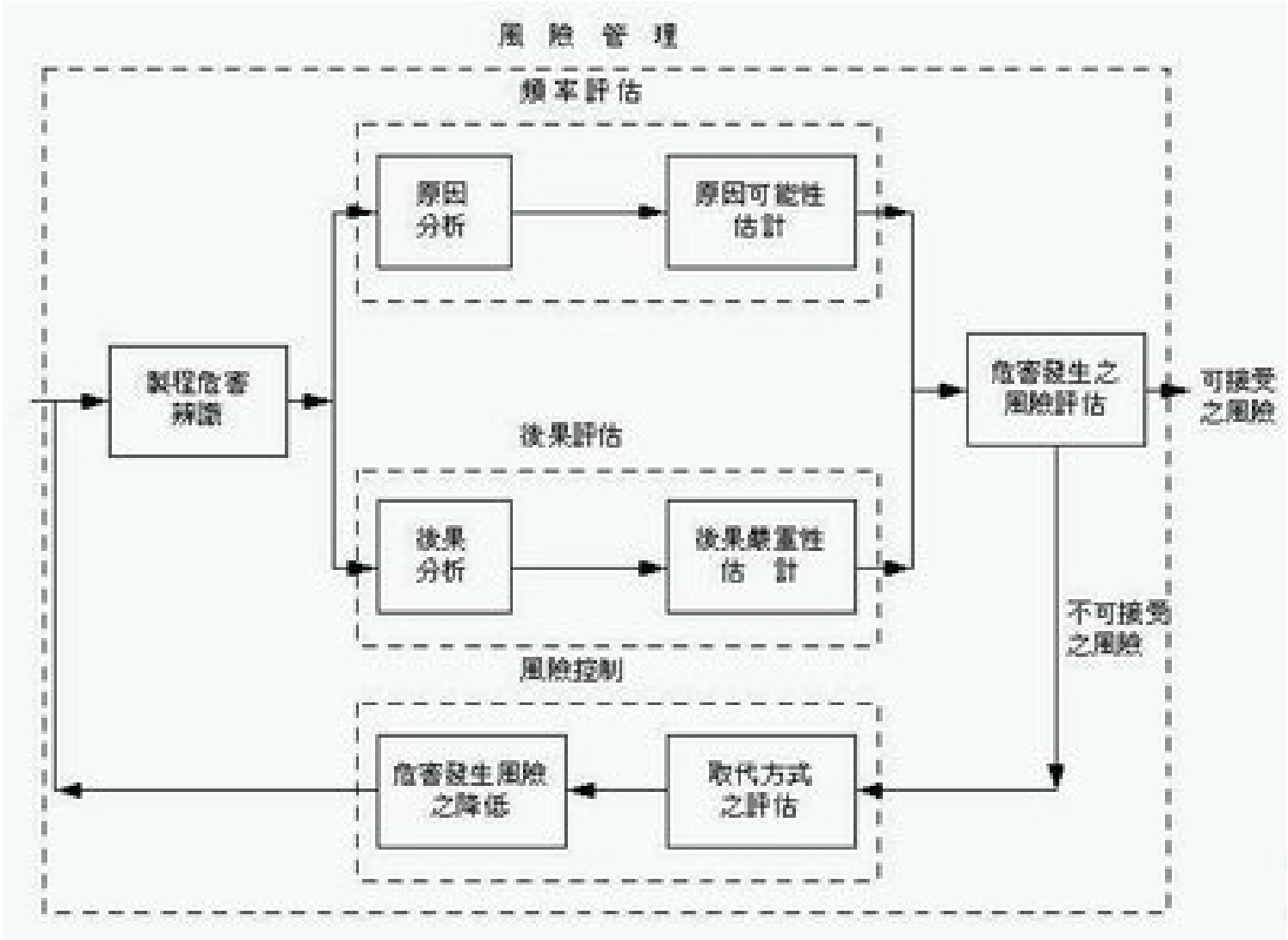
- 系統化分析和管理資訊安全風險的方法。
- 要達到100% 的資訊安全是一種過高的期望，資訊安全管理的目標是透過控制方法，把資訊風險降低到可接受的程度內。



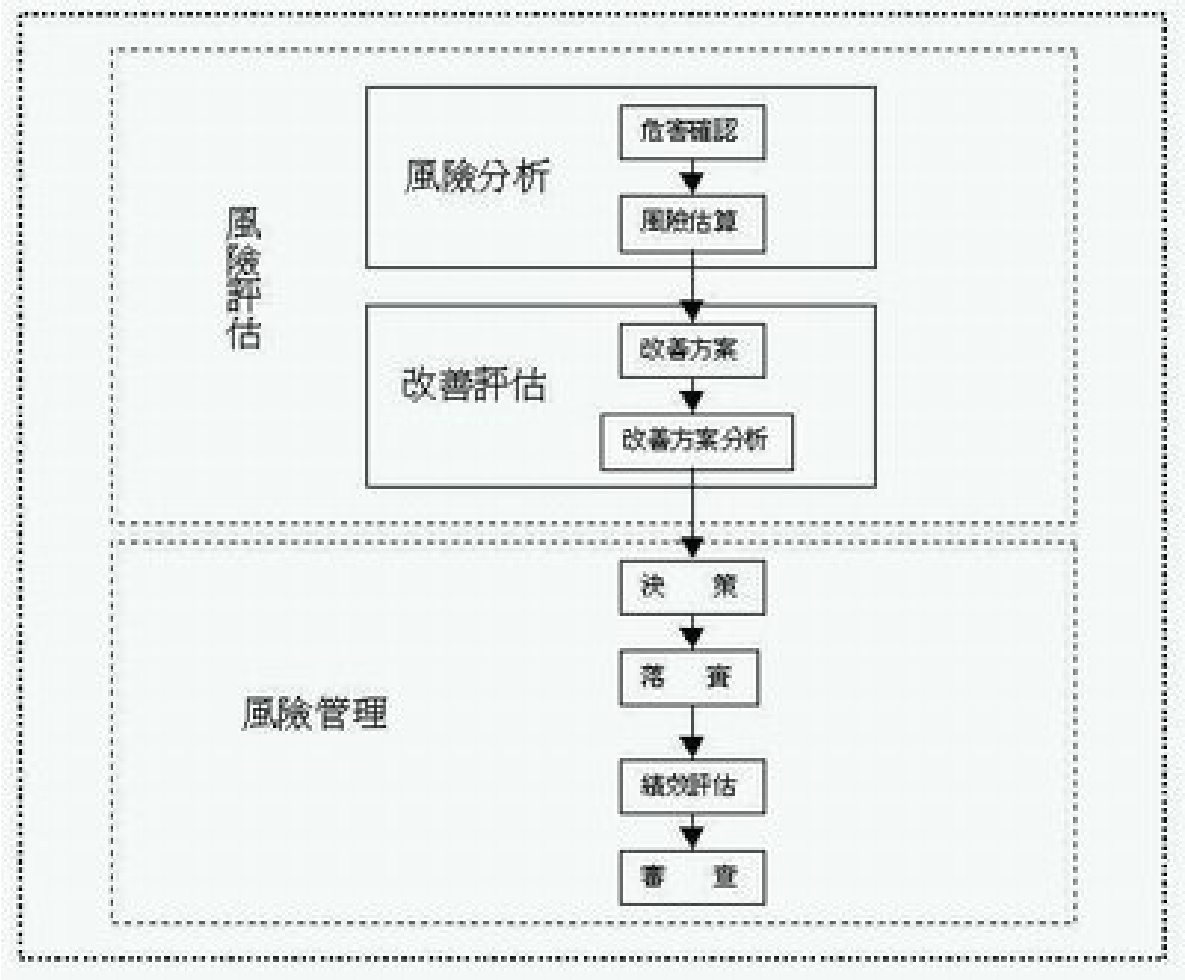
資訊安全管理的三要素



資訊安全的實施—美國模式



資訊安全的實施—加拿大模式



資訊安全的實施

- 無論美國或加拿大模式，大致上都包含了五階段
  - 風險評估(或風險管理分析)
  - 制定防範政策
  - 依政策進行系統維護與補強
  - 人員教育訓練
  - 稽核

資訊安全的實施-稽核

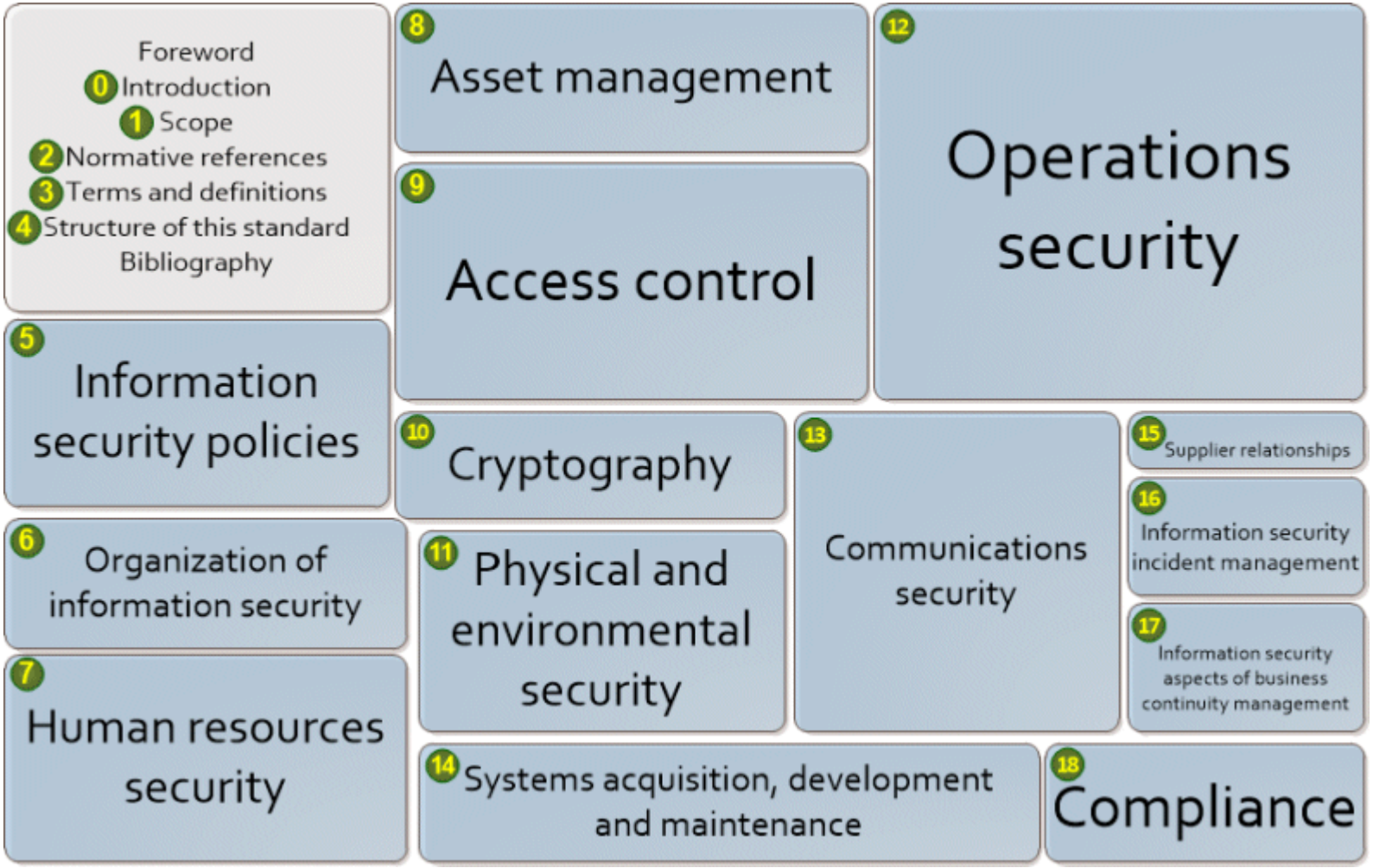
國際與國內資訊安全標準與法令

ISO27001 / ISO27002	資訊安全管理機制
COBIT	國際電腦稽核協會,資訊技術控制架構, http://www. isaca.org/
NIST	美國國家標準與技術協會, http://csrc.nist.gov/nistpubs/800-14.pdf
BIS Basel II	國際清算銀行/新巴塞爾資本管理協定 New Basel Capital Accord
我國政府規範	『行政院所屬各機關資訊安全管理實施基準/要點』『財政部暨所屬機關資訊安全管理基準』『金融機構辦理電子銀行業務安全控管作業基準』
ITIL/ISO20000	英國政府商務部 (Office of Government Commerce) 在 1989 年定的一套 IT 管理方案
Electronic Banking Control	美國聯邦存款保險公司電子銀行控制架構評估—稽核規範
PCI DSS	支付卡產業資料安全標準，處理支付卡相關聯的機構都必須符合該標準的要求。

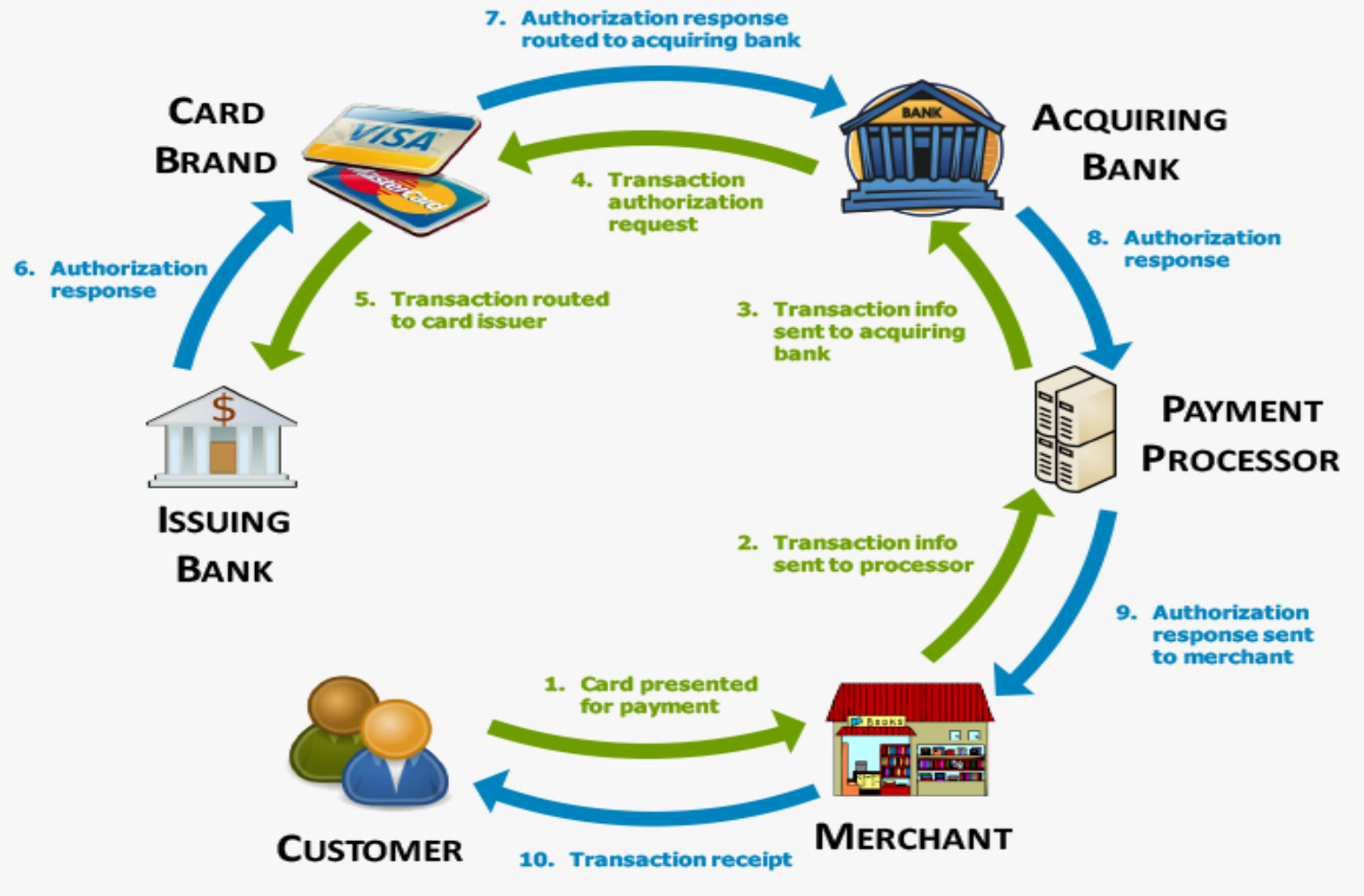
ISO27000系列標準

ISO/IEC 27000	**資訊安全管理系統 - 綜述及詞彙**
ISO/IEC 27001	資訊安全管理系統 - 要求
ISO/IEC 27002	資訊安全管理實踐準則
ISO/IEC 27003	資訊安全管理系統實施指導
ISO/IEC 27004	資訊安全管理系統 - 測評
ISO/IEC 27005	資訊安全風險管理
ISO/IEC 27006	針對審查及認證資訊安全管理系統的實體之要求
ISO/IEC 27007	資訊安全管理系統審查指導（本標準專注於管理系統）
ISO/IEC TR 27008	資訊安全管理系統審查者指導（本標準專注於資訊安全控制）

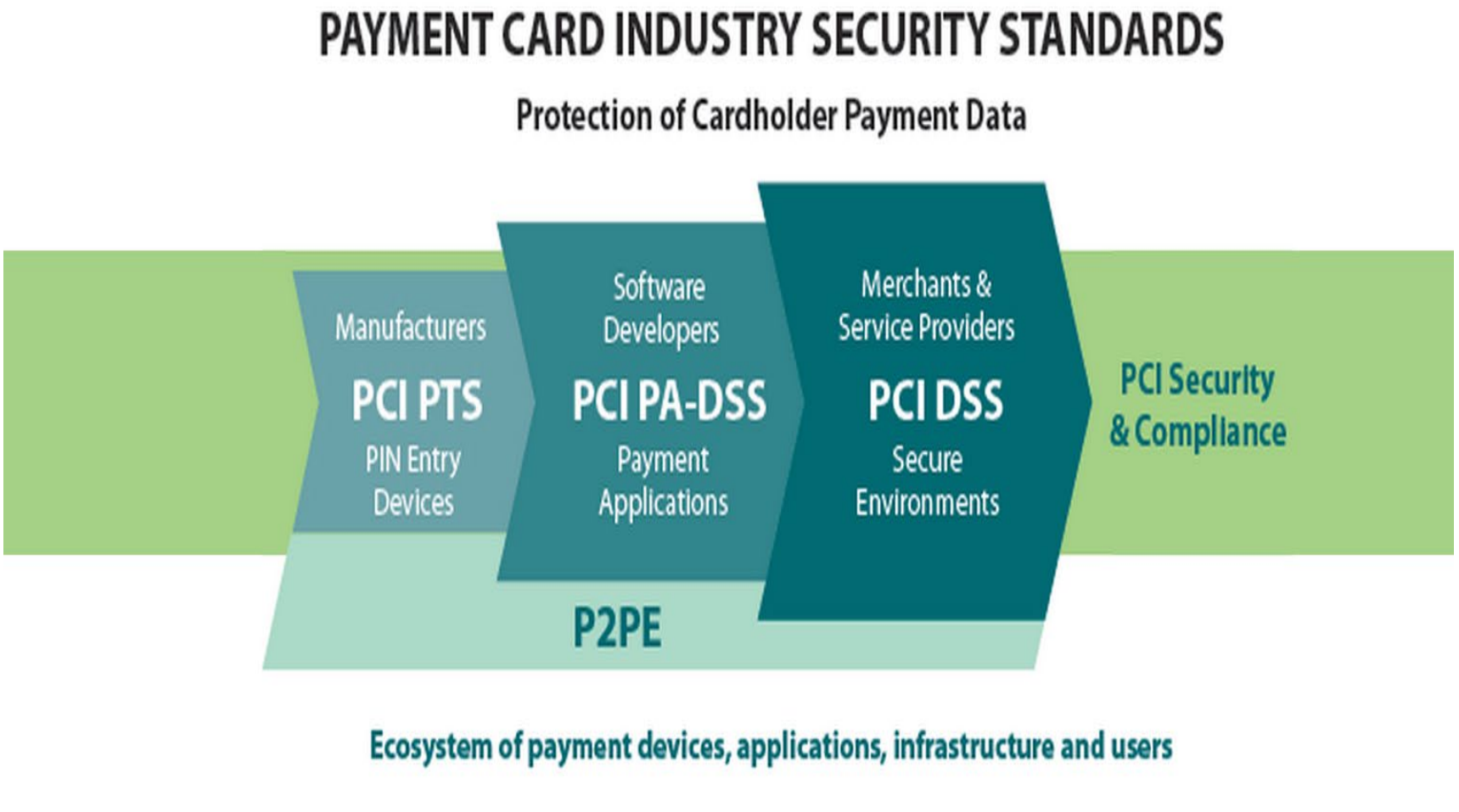
ISO/IEC 27001 控制項目



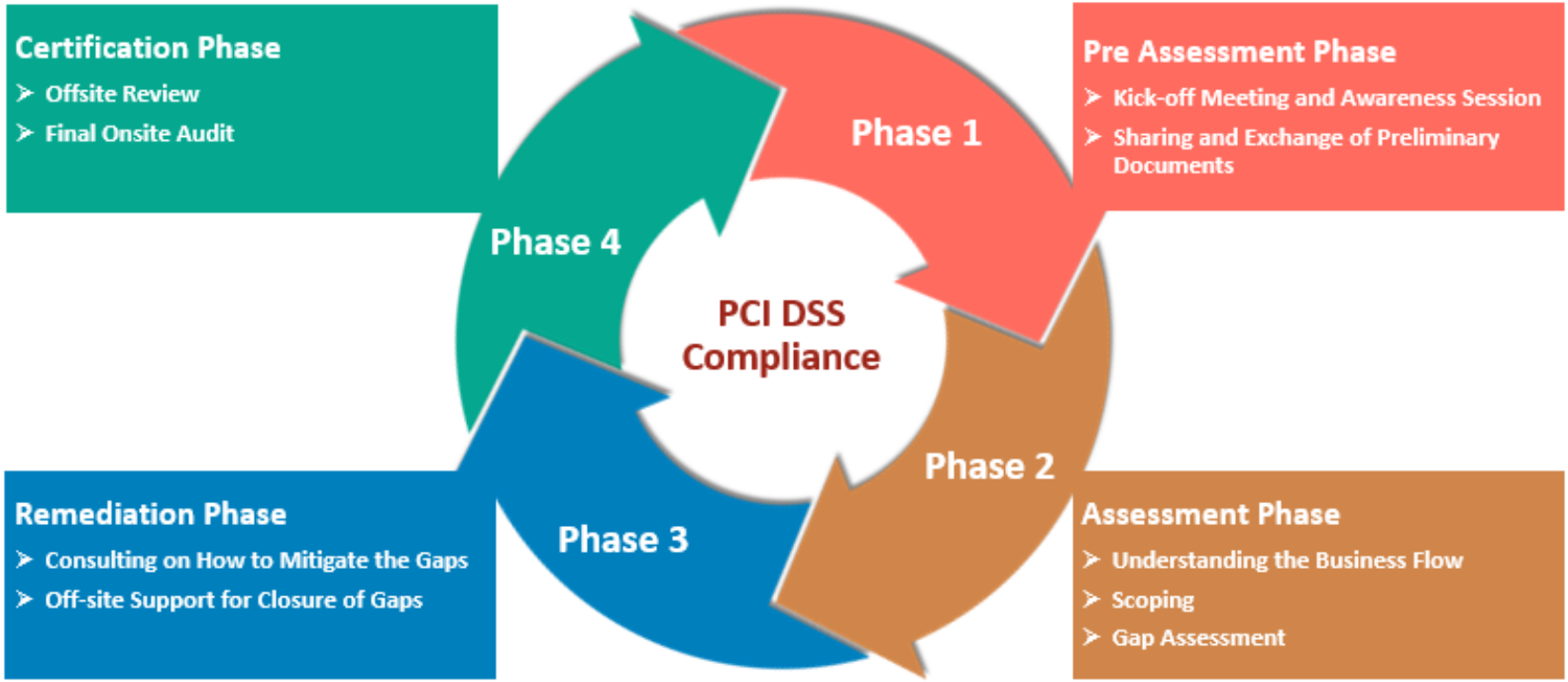
PCI DSS 規範領域


7. Authorization response routed to acquiring bank
CARD BRAND
VISA
BANK
ACQUIRING BANK
4. Transaction authorization request
8. Authorization response
6. Authorization response
5. Transaction routed to card issuer
3. Transaction info sent to acquiring bank
PAYMENT PROCESSOR
ISSUING BANK
2. Transaction info sent to processor
9. Authorization response sent to merchant
1. Card presented for payment
CUSTOMER
MERCHANT
10. Transaction receipt

PCI DSS 相關標準


PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
Manufacturers
PCI PTS
PIN Entry Devices
Software Developers
PCI PA-DSS
Payment Applications
Merchants & Service Providers
PCI DSS
Secure Environments
PCI Security & Compliance
P2PE
Ecosystem of payment devices, applications, infrastructure and users

PCI DSS 遵循性


Certification Phase
Offsite Review
Final Onsite Audit
Phase 1
Pre Assessment Phase
Kick-off Meeting and Awareness Session
Sharing and Exchange of Preliminary Documents
Phase 4
PCI DSS Compliance
Phase 2
Remediation Phase
Consulting on How to Mitigate the Gaps
Off-site Support for Closure of Gaps
Phase 3
Assessment Phase
Understanding the Business Flow
Scoping
Gap Assessment

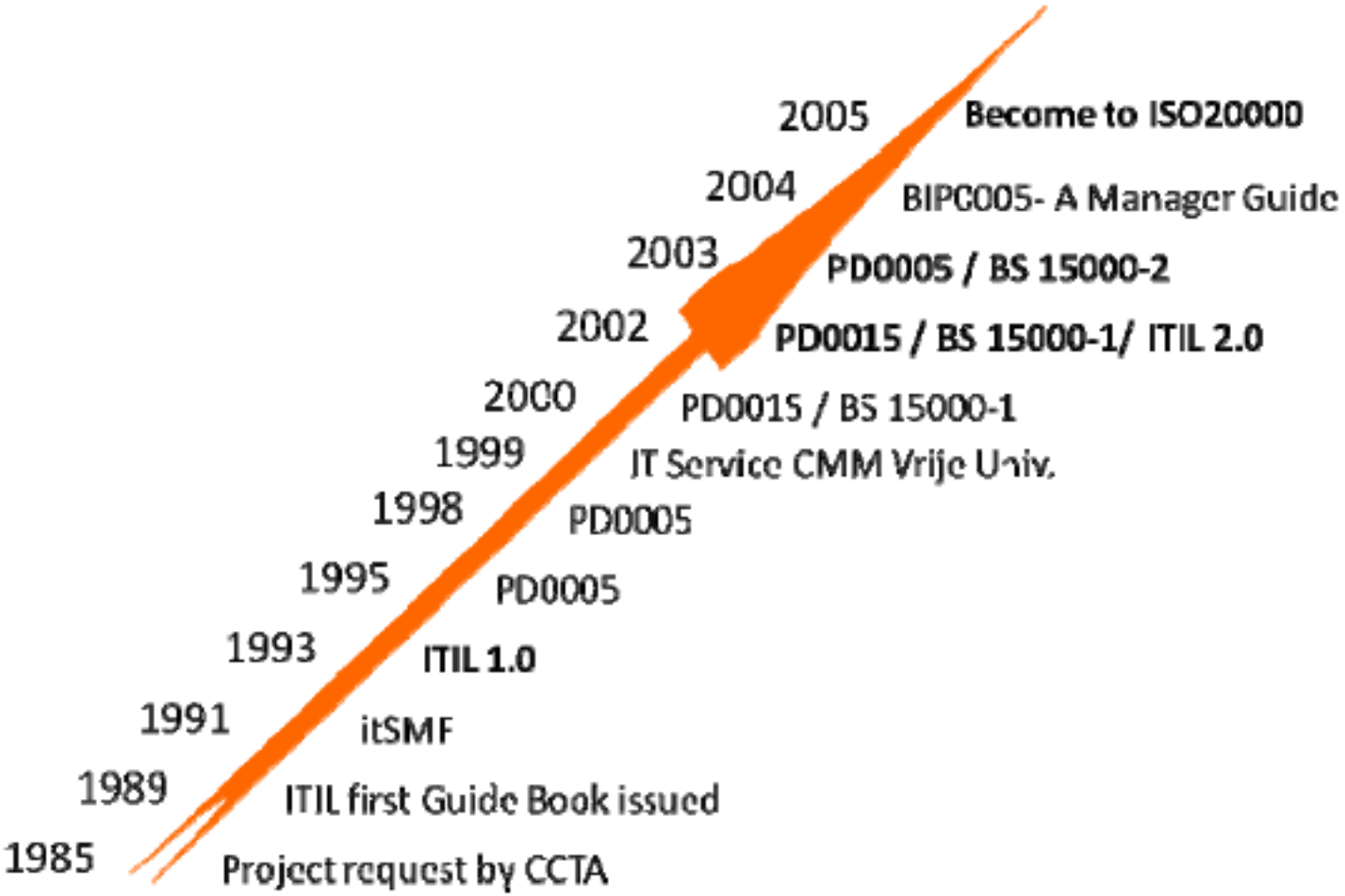
PCI-DSS的規範目標

- PCI-DSS的目的，就是規範具備處理支付卡款項的公司、或是相關的服務提供商(像是第三方支付公司)等，無論服務、網站規模、交易量多寡，都必須透過符合其規範標準，來達到信用卡交易的環節，都不會有外洩或遭竊的風險，具體的六大目的如下：

1. 構建並維護安全的交易系統及網路(Build and Maintain a Secure Network and Systems)
2. 保護交易持卡人數據及資料安全(Protect Cardholder Data)
3. 維護漏洞管理程式(Maintain a Vulnerability Management Program)
4. 執行嚴格的訪問權限控制措施(Implement Strong Access Control Measures)
5. 定期監控並測試服務之網路安全(Regularly Monitor and Test Networks)
6. 維護資訊安全政策(Maintain an Information Security Policy)

ISO/IEC 20000 ITSM架構

ISO20000發展史



資訊安全管理循環

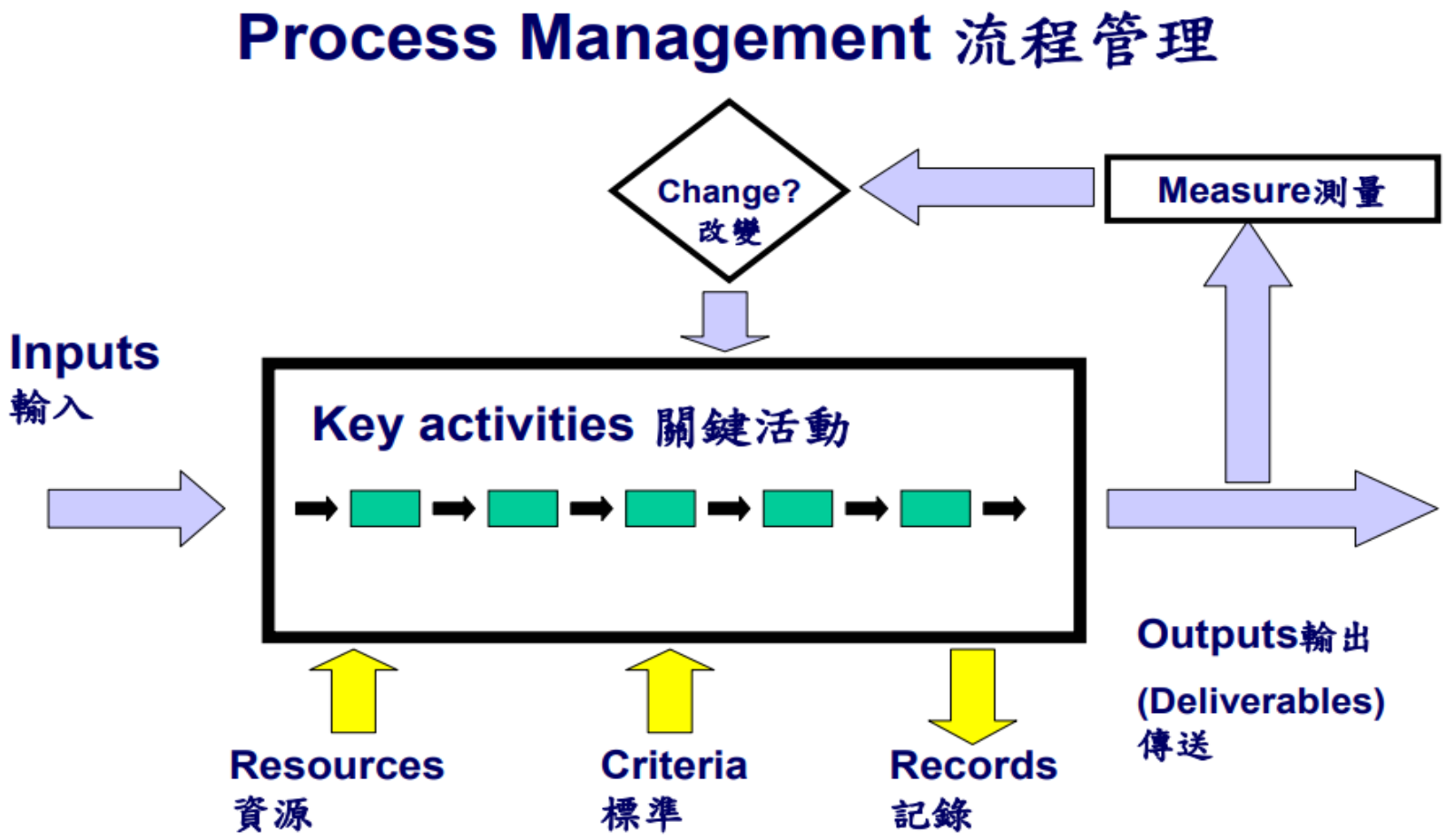
資訊安全管理循環與執行步驟

- 確定範圍
- 資訊資產鑑別及價值確認
- 資訊資產風險評估
- 擬定資訊政策及資訊安全制度
- 控制目標及控制程序鑑定
- 落實執行資訊安全管理系統
- 定期稽核及持續性改善

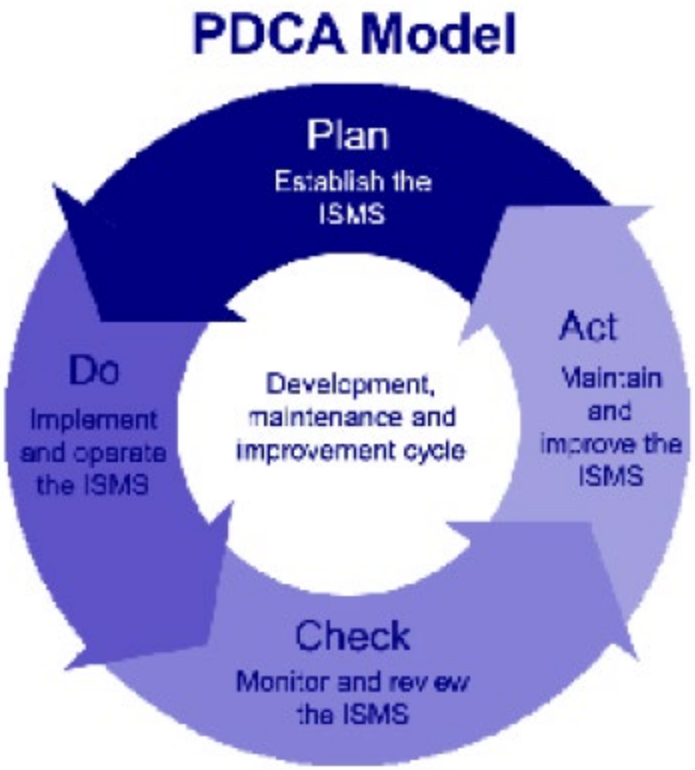
流程導向 (Process Approach)

- 標準倡導以『流程導向』來開發、執行及改進組織資訊安全管理系統效能。
- 何謂流程導向？
  - 組織必須鑑別、管理許多活動方能有效運作。使用資源 與管理，將輸入轉換為輸出之活動，可視為一個流程。
  - 通常一個流程之輸出可直接地成為下一個流程之輸入。
  - 組織必須妥善管理各流程，包括各流程之鑑別與相互作 用，使其有效運作，達成組織營運目標。

流程導向管理


Process Management 流程管理
Change?
改變
Measure測量
Inputs
輸入
Key activities 關鍵活動
Outputs輸出
(Deliverables)
傳送
Resources
資源
Criteria
標準
Records
記錄

資訊安全管理系統的方法論



Plan
- Define the ISMS scope and the organization's security policies
- Identify and assess risks
- Select control objectives and controls that will help manage these risks
- Prepare the statement of applicability

Do
- Formulate and implement a risk mitigation plan
- Implement the previously selected controls in order to meet the control objectives.

Check
- Perform monitoring procedures
- Conduct periodic reviews to verify the effectiveness of the ISMS
- Review the levels of acceptable and residual risk
- Periodically conduct internal ISMS audits

Act
- Implement identified ISMS improvements
- Take appropriate corrective and preventive action
- Maintain communications with all stakeholders
- Validate improvements

資訊安全管理系統- Plan

- 訂定適用範圍
- 定義ISMS管理系統政策
- 建立系統化的風險評鑑方法
- 鑑別各項風險
- 評鑑各項風險
- 鑑別並評估風險處理之選項及方法
- 對各項風險選擇控制目標及控制程序
- 擬定適用性聲明書（SOA）

資訊安全管理系統- Do

- 系統化陳述風險處理計畫
- 實施風險處理計畫
- 實施控制措施符合管制目標
- 實施訓練及認知計畫
- 作業管理
- 資源管理
- 實施安全事件回應處理作業程序
- 其他控制措施

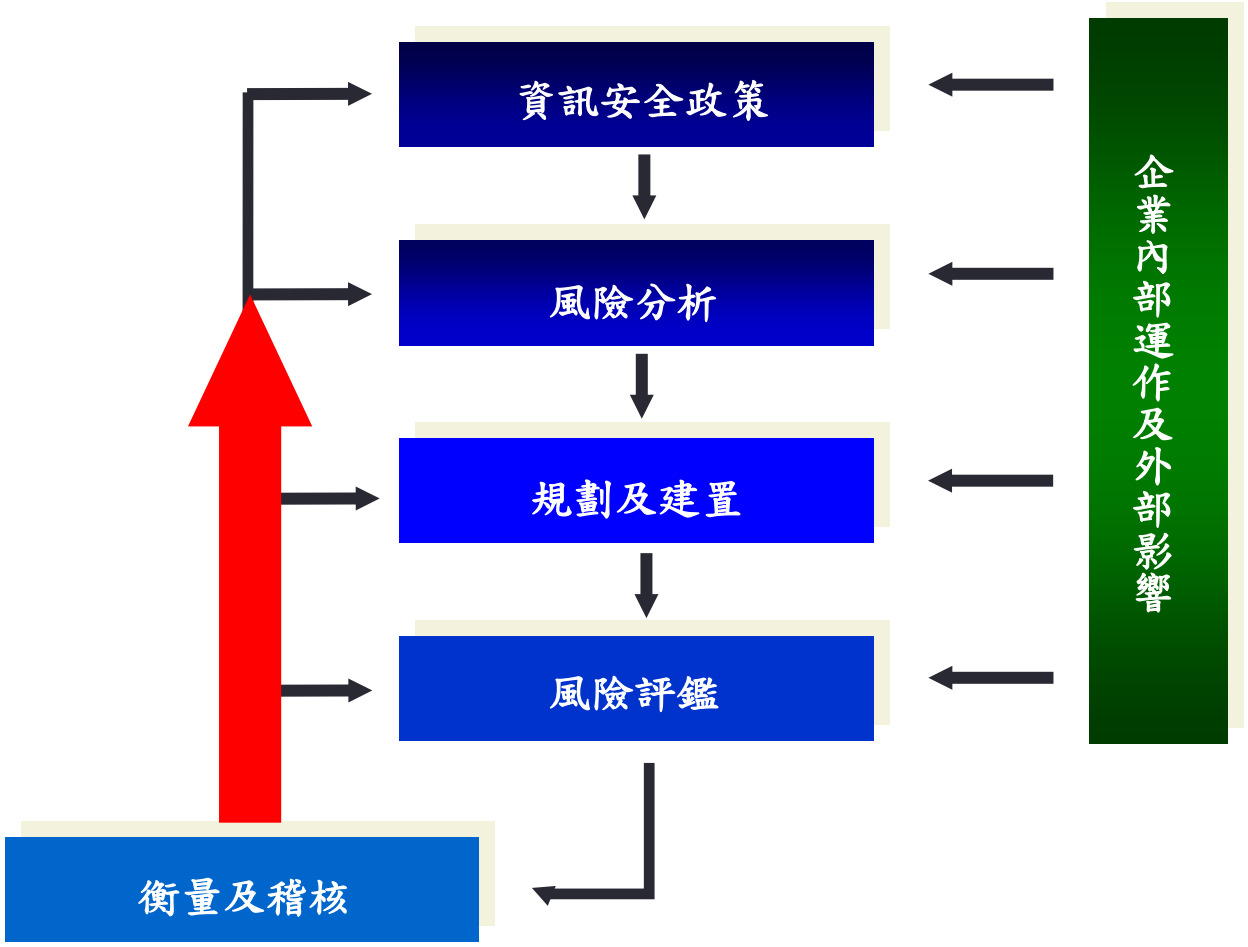
資訊安全管理系統- Check

- 監控程序及其他控制措施
- 定期審查有效性
- 風險監控-殘餘風險與可接受風險等級
- 執行稽核(遵循性)
- 紀錄影響行動與事件

資訊安全管理系統- Act

- 維持及改善資訊安全管理系統
  - 執行改善活動
  - 矯正及預防措施，
  - 組織本身知安全經驗
  - 汲取其他組織或
  - 利害相關團體對各項措施進行溝通
  - 確保各項措施達到預期目標

ISMS管理流程



ISMS範圍定義

- 建置範圍之辨識與確認
  - 確認ISMS建置時可能影響的範圍
  - 避免因未確認範圍而導致專案無限擴大
  - 避免無法判斷資訊資產及風險等
  - 避免增加專案執行之風險
  - 為使ISMS建置專案能順利推展

資產

- 組織資源、程序、產品、資訊架構等有形或無形項目
  - 實體資產：實體資訊設備
  - 資訊類資產：電子形式存在資訊資產
  - 文件資產：以書面形式存在的資訊
  - 軟體資產：作業系統及應用系統等組織營運使用到的軟體資產
  - 人員：管理及使用資訊資產的相關人員
  - 服務：網路服務、電力、機房空調等維續營運環境運作的其它資產

資產鑑別及價值確認

- 資產鑑別及價值確認
  - 有形的價值：購買成本,建置成本,維護成本,復原成本,停機時間損失.....
  - 無形的價值：商譽損失,信用損失.....
- 資訊分類
  - 以下有幾個很好的原因來解釋為何要分類資訊。對於組織來說，不是所有的資訊都有同等的價值。有一些資訊
  - 例如商業機祕、公式和是新的產品資訊等有價值的資訊外流時，將會造成企業體在市場中很嚴重的問題，例如造成大眾困窘或造成不信任。

資訊分類的益處

- 顯示一個組織的對安全保護的義務。
- 幫助識別那一個資訊對組織來說影響最大或最重要的。
- 支持機密性、完整性以及可用性原則
- 幫助識別那一個保護可以適用於那一個資訊。
- 可用來規定、條款或是法律用途

資訊分類範例~1

- 不保密、未經分類的unclassified information：無任何敏感度或不須分類的資訊。這個資訊是由大眾所釋放的，不會損及機密。
- 敏感但未經分類的(SBU)：此資訊有很小影響力的機密，且如果流露出去的話，並不會造成太大的傷害。例如考試的答案就為此種資訊，或是保健資訊為另一例子。
- 機密confidential ：資訊本身就有機密性。而未經授權的流露出此種資訊會造成一些國家安全的損傷。此種程級為歸檔為敏感度SBU或是極機密之間。
- 極機密secret：資訊本身極機密。未經授權的流露出此種資訊會造成國家安全的嚴重損傷。
- 最高機密top secret：最高程度的資訊分級(基本上，只有美國的總統能知的程度)。未經授權而流露出的最高機密資訊將會國家安全造成無可預計的重大損失。

資訊分類範例~2

- 公眾：此類資訊與未經分類的(unclassified information)的資訊雷同;所有公司的資訊不屬於下一個種類的是屬於此公眾資訊。此種類料可能不會發佈，但一經發布也不會有太嚴重或不利地影響公司。
- 敏感：此種資訊須要比平常的資訊分類在更高等級。而且須要防止機密的流失和因為未經授權的修改而損及原始性。
- 私人：此類資訊屬於私人資訊而且僅供公司使用。如果散佈出去的話可能對公司或員工造成不利。例如，薪水的等級和病史皆屬於私人資訊。
- 機密：此類資訊敏感度高而且僅供內部使用。而且須免除發佈，並在資訊發佈條款(Freedom of Information Act)之下。

資訊分類角色

- 擁有者
  - 資料的擁有者可能會是組織的的執行人員與經理。而他將要對公司的資料資產負責及保護。資料擁有者與監護人是不同的，擁有者擁有對資料保護的最後法人責任，且如果因為輕忽而無法保護這些資料時，須對此全部的負責。但每日實際的運行職務是屬於監護人的。
- 監護人
  - 擁有者將保護資料的權責委託給監護人， IT系統人員通常執行此角色。
- 使用者
  - 在資料分類政策裡，使用者可以是任何的一個人(例如操作員、雇員、或是外部關係人)他的部份工作涉及反覆的使用此資料
- 系統稽核員：(Information systems auditors)
  - 他們的須要提供報告給高級管理人員，他們須處理常態性工作、獨立審查，這些都是為了使安全控管更效率。他們也檢視安全政策、標準、指導方針、和程序有無遵從公司的目標和方針。

營運衝擊分析

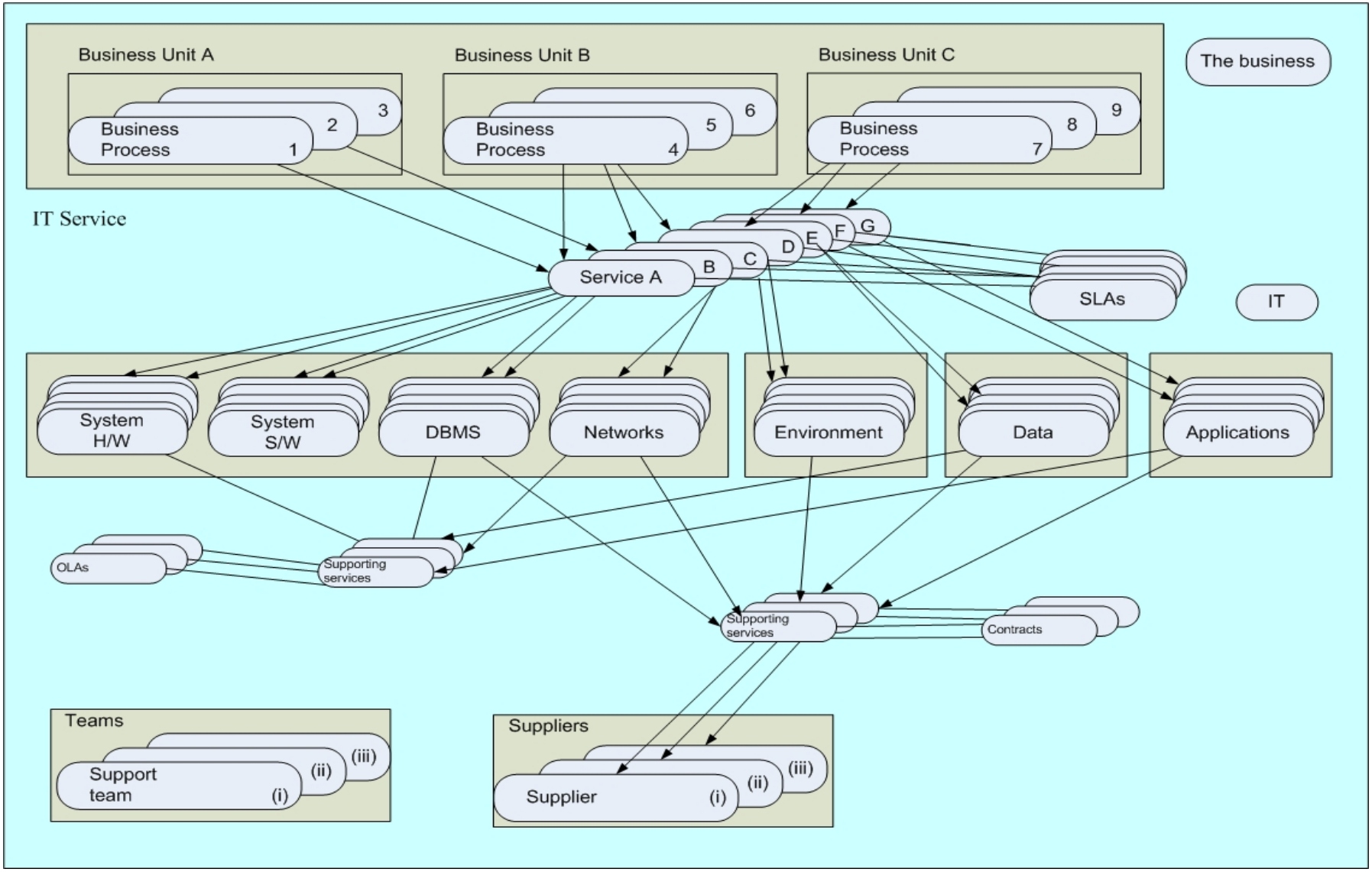
- A management level analysis that identifies the impacts of losing the entity’ s resources. This analysis measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions concerning hazard mitigation, recovery strategies, and continuity planning. 管理階層對於辨識喪失機構（entity）資源造成的衝擊分析。此分析衡量資源喪失的影響和隨時間累計的損失，並提供機構可靠的資料，以作為降低危害、復原策略和持續計畫決策的基準。（NFPA1600）
- The organization should determine and document the impact of a disruption to the activities that support its critical products and services. This process is commonly referred to as a business impact analysis. 組織應決定及提供中斷支援其重要產品與服務活動衝擊的文件。（ISO 22301）

營運衝擊分析(續)

識別核心業務流程

識別核心系統與關鍵元件

識別業務影響與可容忍等級



Source: OGC ITIL Service Design V3

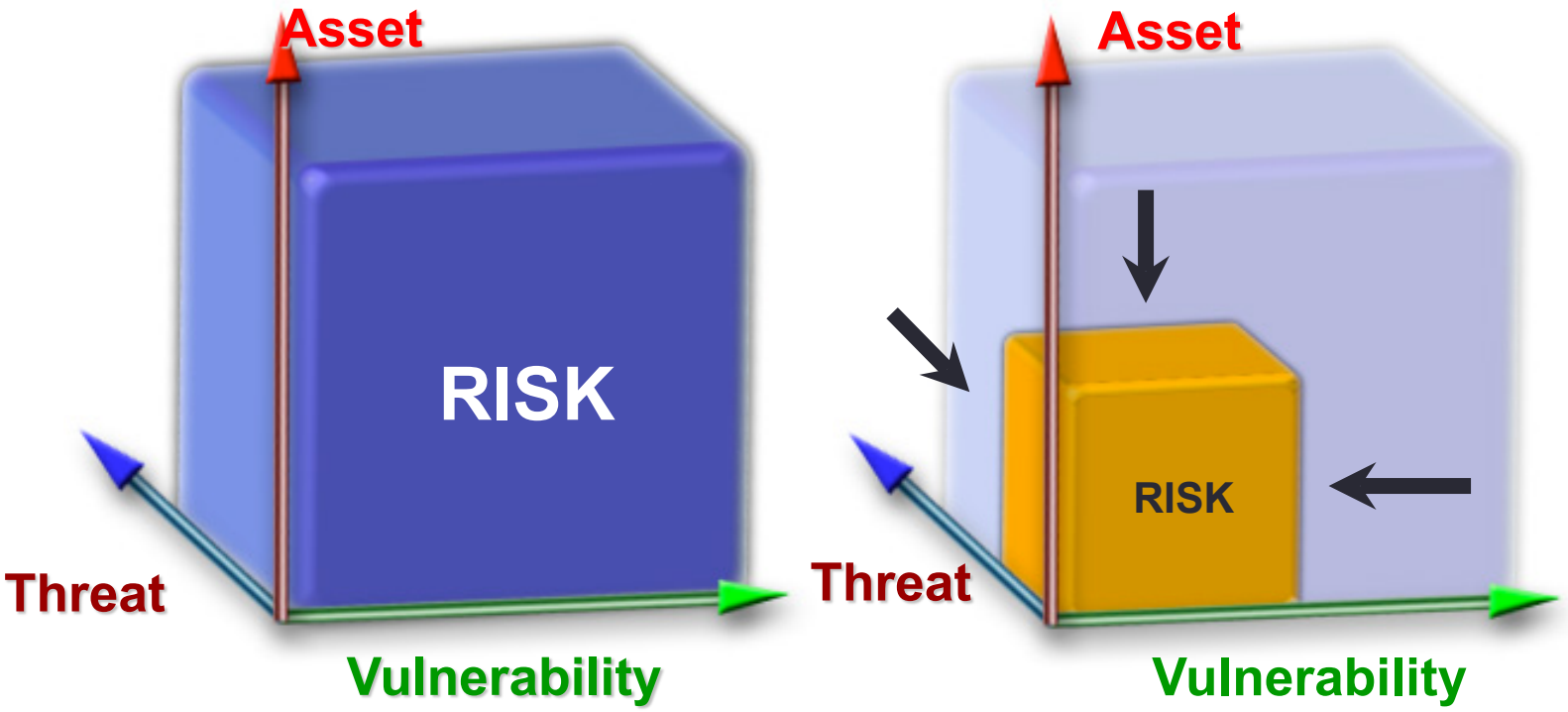
服務層級協議 (Service Level Agreement；SLA)

- 服務層級協議(Service Level Agreement；SLA)指的是服務提供者與使用客戶之間，應就服務品質、水準以及性能等方面達成協議。在設立SLA時，服務提供者首要之務，就是與使用者達成共識，決定整體方法與指導原則，並加以標準化。

風險評估與管理定義

- 風險評估(Risk Assessment)
  - 對於資訊資產所遭受的威脅(threat)、存在的安全缺陷(vulnerability)、造成的衝擊(impact)及發生頻率(occurrence)的可能性(likelihood)所作的評估。
  - 風險評估的結果可幫助指導應採取的合適管理措施，判斷各種不同風險的管理優先順序，決定應該使用那些控制，以降低風險
- 風險管理(Risk Management)
  - 在可接受的成本下，對於風險所進行的辨明(identifying)、控制(Controlling)、最小化(minimizing)或消除(eliminating)之管理過程

資訊安全風險評鑑與管理



管理資訊風險的策略與決定因素

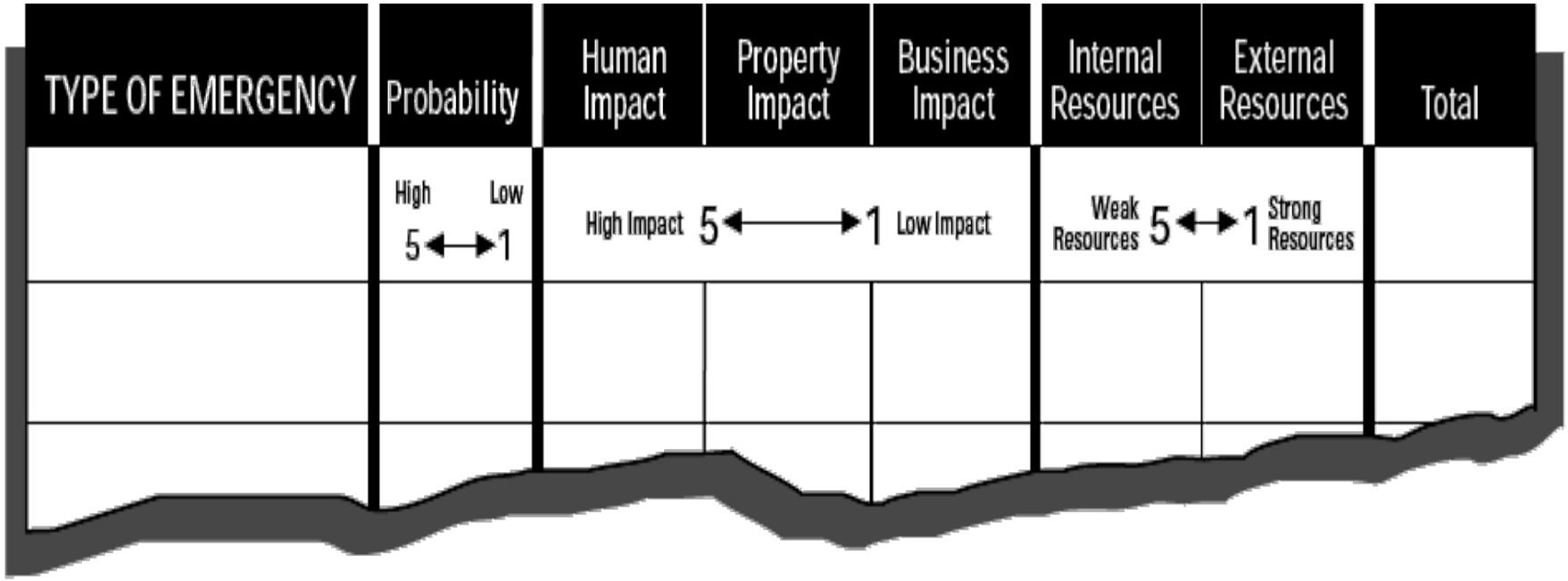
- 管理資訊風險的策略
  - 接受風險
  - 規避風險
  - 轉移風險
  - 降低風險
- 管理風險的決定因素
  - 業務需求
  - 成本考慮
  - 法令要求

風險評估表格(矩陣表)

RISK MANAGEMENT			
No	Threat	Description of the risk	Comment
1	Hackers		
2	Information theft		
3	Industry espionage		
4	Virus		
5	Intentional erasure		
6	Unintentional erasure		
7	Awareness		
8	Power failure		

風險評估(Risk Assessment)

- 風險評估評分範例



定量化風險分析
（Quantitative risk Analysis）

Ranking value	Probability	Impact (thousands of dollars)	When needed (weeks)	Cost to implement (thousands of dollars)	Likelihood of control working
125.025	0.5	500	1	2	0.5
83.596	0.84	200	4	4	0.33
37.64	0.33	200	2	20	0.84
4.9816	0.33	30	4	3	0.84

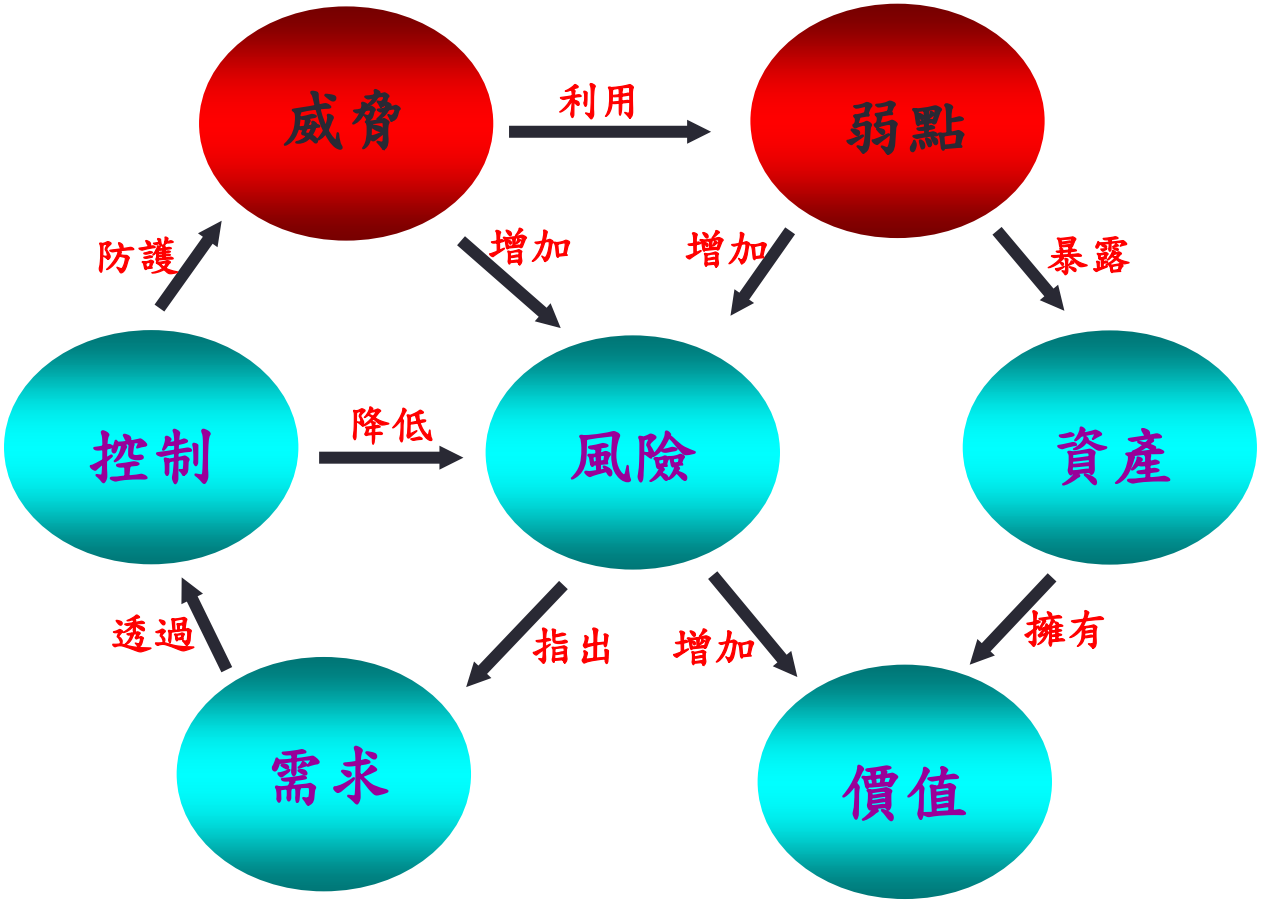
機率與衝擊矩陣

Impact

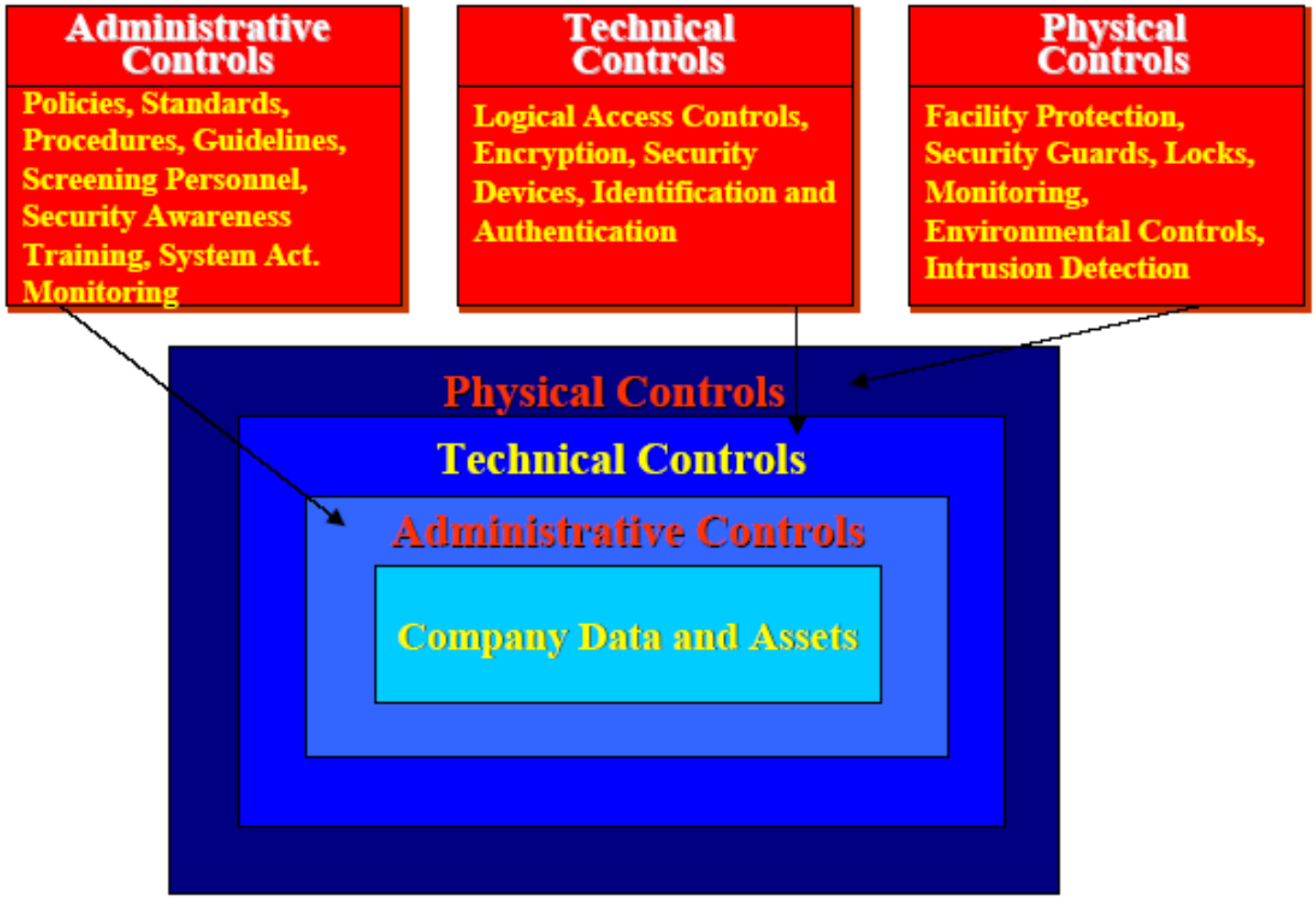
Probability

	Insignificant	Minor	Significant	Damaging	Serious	Grave
Negligible	Nil	Nil	Nil	Nil	Nil	Nil
Very Low	Nil	Low	Low	Low	Medium	Medium
Low	Nil	Low	Medium	Medium	High	High
Medium	Nil	Low	Medium	High	High	Critical
High	Nil	Medium	High	High	Critical	Extreme
Very High	Nil	Medium	High	Critical	Extreme	Extreme
Extreme	Nil	Medium	High	Critical	Extreme	Extreme

風險評鑑



控制項目


Administrative Controls
Policies, Standards, Procedures, Guidelines, Screening Personnel, Security Awareness Training, System Act. Monitoring
Technical Controls
Logical Access Controls, Encryption, Security Devices, Identification and Authentication
Physical Controls
Facility Protection, Security Guards, Locks, Monitoring, Environmental Controls, Intrusion Detection
Physical Controls
Technical Controls
Administrative Controls
Company Data and Assets

控制項目的目的

- 資安事件的預防(Preventive)
- 資安事件的偵測(Detective)
- 資安事件的回應(Corrective)
- 安全控制應該建立於***預防(Preventive)***

資訊安全成本

- 虛擬成本=發生事故損失成本(L_0)*發生機率(P_0)
- 實際成本=改善資通安全所花費之成本
- 改善前資通安全成本(B)= L_0*P_0
- 改善後資通安全成本(A)= L *P_1
  - P_1(改善後發生機率)
- 有效改善 B > A

資訊安全的實施-防範政策

- 評估完成後，便是政策與程序的制定
- 防範政策的訂定與改善程序將直接影響資通安全成本
- 政策制定後，並非一成不變，必須由風險改善程度而調整政策之內容

資訊安全的實施-防範政策

- 防範政策至少須具有以下內容：
  - 資訊使用政策
  - 網路管理政策
  - 系統維護政策
  - 帳號密碼管理原則
  - 備份計劃
  - 緊急應變計劃
  - 災難復原計畫

資訊安全的實施-系統維護

- 系統維護內容應包含
  - 危機通報系統
  - 緊急應變通訊系統
  - 網路安全防範
    - 防火牆
    - 虛擬私人網路(VPN)等機制
    - 入侵偵測系統(IDS)
  - 人員身分管理系統
  - 加密
    - 金鑰管理
    - 演算法
  - 實體安全
    - 火災，高溫，斷電等事故的保護

資訊安全的實施-教育訓練

- 員工
  - 使其能對機關產生認知意識，並能保護機關內部機密資訊
- 系統維護者
  - 提昇其資通安全之基本技能，了解最新的駭客技術、安全威脅、安全修補等資訊
- 管理階層
  - 在教育訓練過程中了解各部門在資通安全中所扮演的角色
  - 實施資通安全的基礎課程，以能確切制定防範政策

資訊系統稽核歷史

- 資訊系統稽核在早期是傳統會計審計業務的一部分
- 主要關注於被稽核單位的電子資料取得、分析與計算等資料處理業務
  - 對交易金額、帳戶、報表餘額進行檢查
  - 對客戶的電子化會計資料進行分析處理

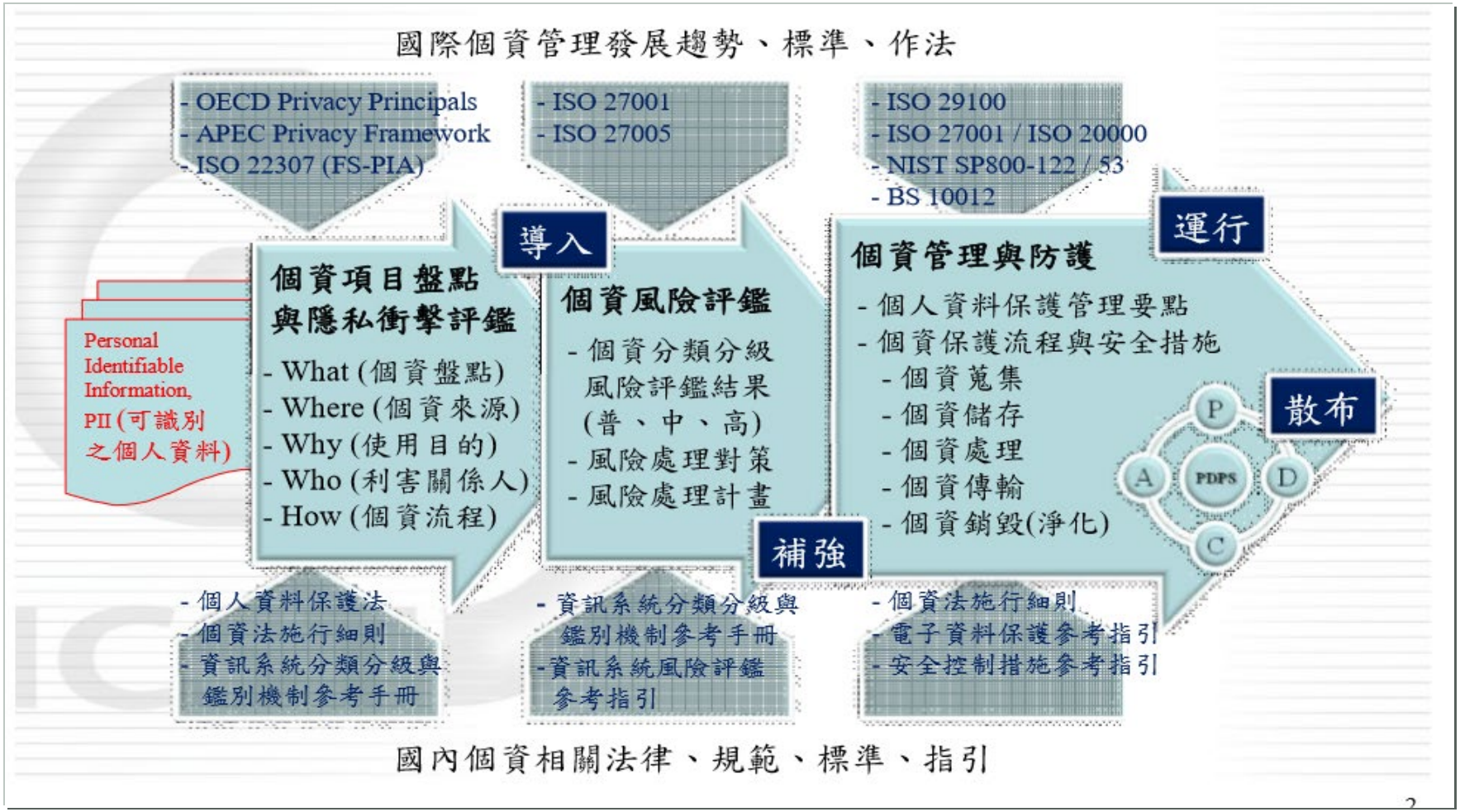
課程大綱

- 近年來網站側錄以及個資外洩案例
- 資訊保護與個人隱私重要性
- 資訊安全管理系統說明
- 個資保護管理制度介紹

個資法防護關鍵及說明

- 除個資法內明訂之特種個資外(敏感性個資)其餘個人資訊還是可以合理使用。
- 當必須蒐集處理或利用個資時必須符合法律及相關規定，但最重要是必須保護及存放相關紀錄以便舉證。
- 傳輸及交付個資時必須符合法律及相關規定，但最重要是必須保護及存放相關紀錄以便舉證。
- 關鍵時具效力相關紀錄及舉證。

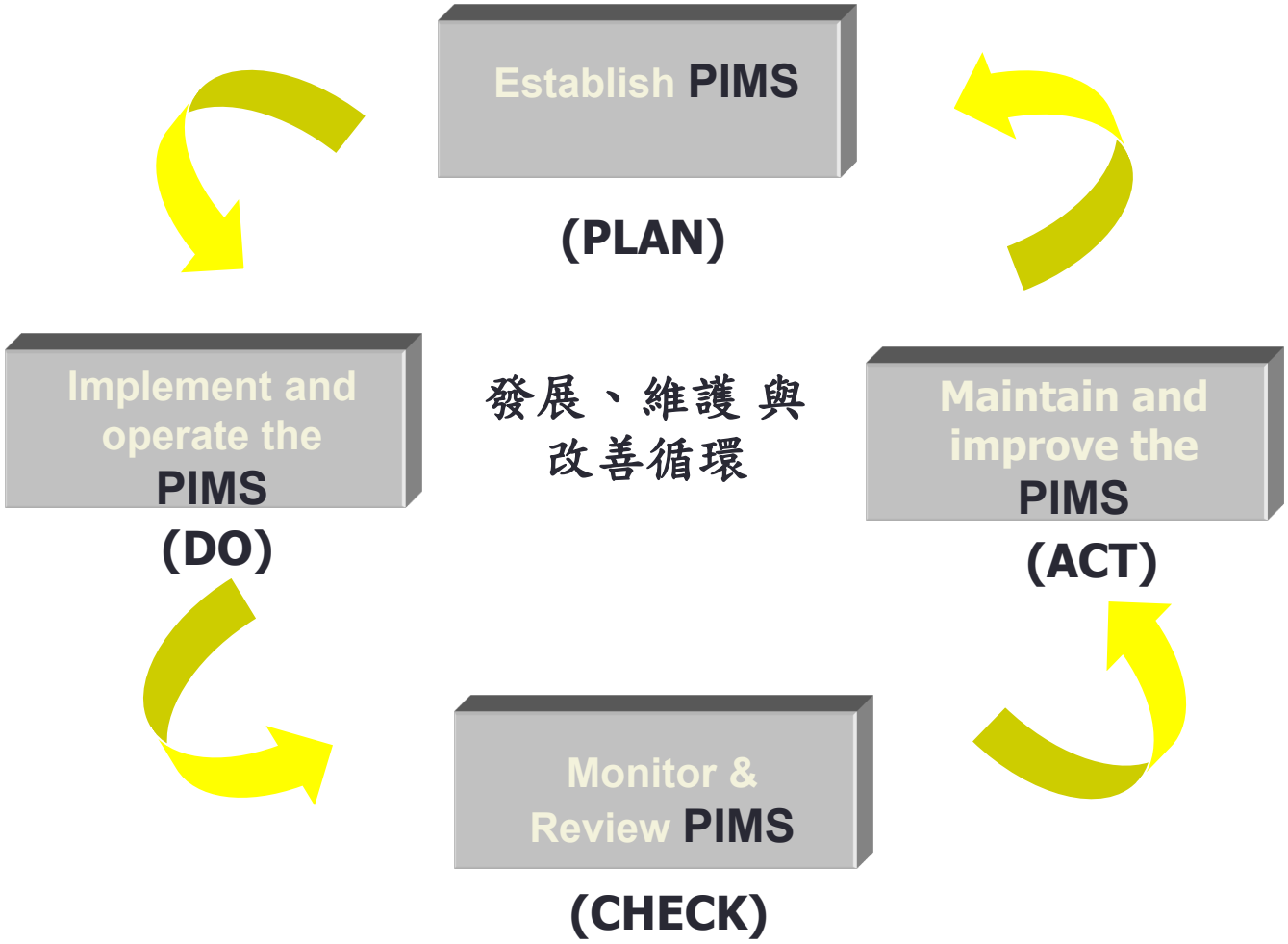
國際間個資管理的發展趨勢



個人資訊管理及防護

- 建立Personal Information Management System (**PIMS) (BS 10012 標準)**
- **主要內**容依照；
  - **Plan(規劃) → Do(執行) → Check(檢查) → Act(行動)的順序**

PIMS建置符合PDCA模型



ISMS與個資防護補強

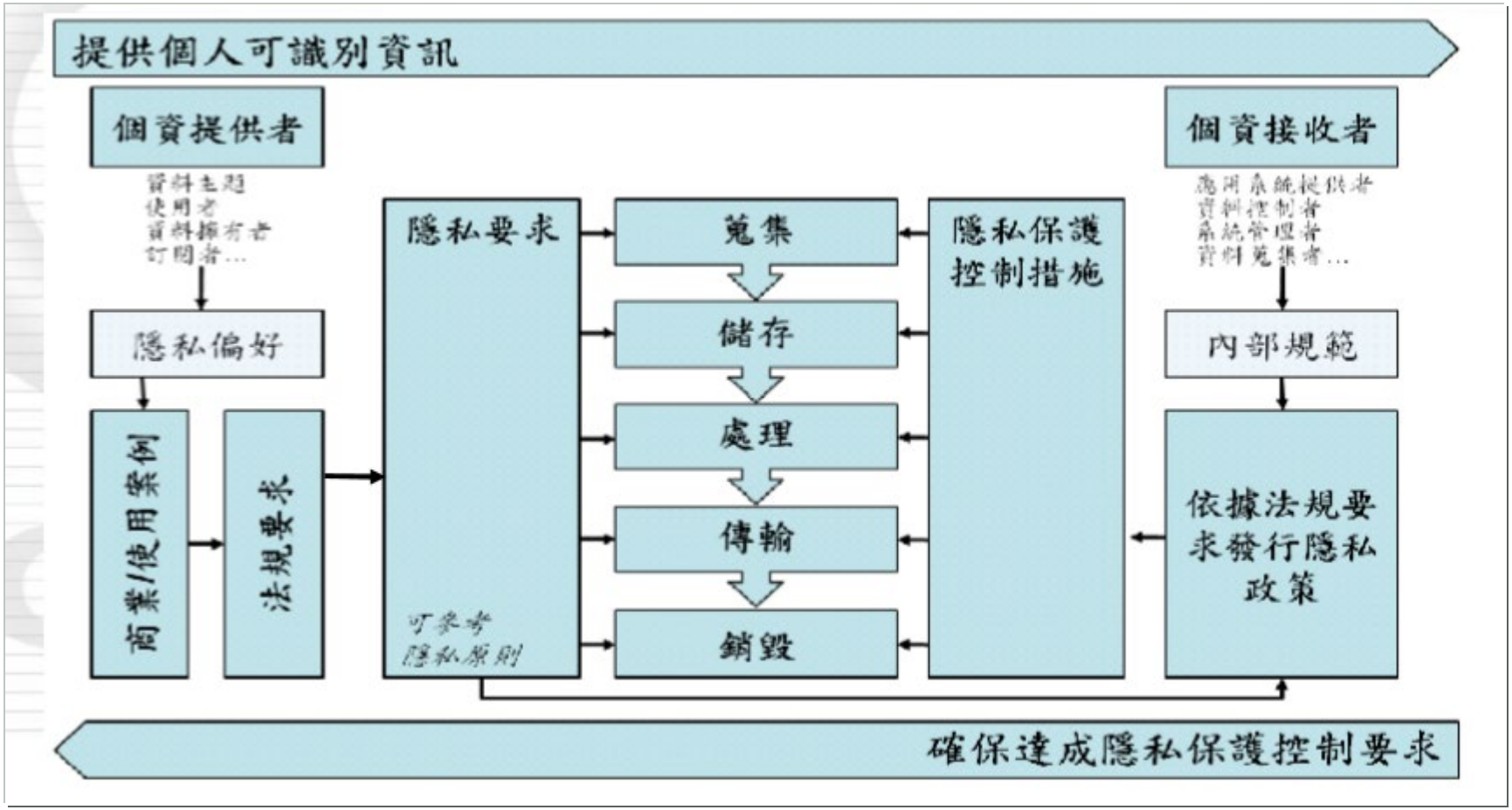
- 資訊安全管理ISMS與個資防護補強
  - ISMS(ISO27001標準) 所著重的部分大多都在於個人資料的”處理”階段。
- 個資法會要求保護個人資料的蒐集、處理、利用、銷毀及國際傳輸
  - 因此在既有的ISMS安全控制措施基礎以上，必須補強個資項目在其他相關生命週期活動中的安全控制措施

個資防護重點與管理

- 個資防護重點
  - 進行個資流程與個資項目盤點
  - 分析個資風險評鑑威脅與弱點
  - 設定流程技術控制措施基準點
- 個資防護管理
  - 組織內部個資管理單位
  - 作業委外個資管理單位

ISO 29100隱私架構

- 公布日期: 2011年12月5日。 規劃個資提供者與接收者之間，有關個資蒐集、儲存、處 理、傳輸及銷毀等作業流程內容



BS 10012:2009(1/2)

- 公布日期：2009年5月 主要依循自英國資料保護法，應用「Plan」、「Do」、「Check」及「Act」循環 ，提供一個保持與提升符合資料保護之法規與良好實踐之架構
- 規劃PIMS(Planning for a Personal Information Management System)：
  - –定義組織中PIMS的範圍與目的：例如建立個人資料保護要點
  - –建立個資管理政策：政策應聲明適用範圍，例如全組織或部分單位
  - –指派適當人員角色職責：例如指派一至多位專業人員負責平時運作
  - –提供足夠的資源：組織在建置、實施、運作及維護PIMS過程中，應提供所需的資源
  - –將PIMS與組織文化契合：例如與組織現有的管理制度、程序進行整合運作，降低對人員日常作業的衝擊影響
- 建置與運作PIMS ：
  - –指派負責人員：確保組織依據其個資管理政策，指派適當的負責人員
  - –識別與記錄個資的用途：個資之識別可從業務流程或服務目錄著手，主要辨別個資 對於流程與活動利害關係人的風險，分析個資的類別，在其不同生命週期的型態、 相關文件、支援系統及彼此間的介面，做為後續風險評鑑的重要輸入來源
  - –教育與認知：確保所有人員能夠認知其在處理個資時的職責

BS 10012:2009(2/2)

- –風險評鑑：確保組織認知當在處理特定類型的個資時之相關風險
- –其他PIMS日常運作活動：包括公平與合法的處理個資、告知流程、維持PIMS為最新狀態、當事人權利、個資保留與銷毀、委外處理流程、對第三方揭露、安全議題及資料正確性等資料
- 監督與檢視PIMS ：
  - –內部稽核：例如稽核規劃、稽核員選擇及稽核要求等
  - –管理審查：審查項目應來自個資管理系統使用者之回饋意見、人員所發現並呈報之風險、稽核結果、程序審查紀錄、技術升級或更換的結果、主管機關的正式評鑑要求、抱怨處理及已發生的違反安全事故等
- 改善PIMS ：
  - –預防措施與矯正行動：所有變更或改善的建議，應於實施前進行評估，以符合政策上的要求
  - –持續改善活動：透過稽核結果、矯正預防措施及定期檢視的作法，以持續改善PIMS的有效性

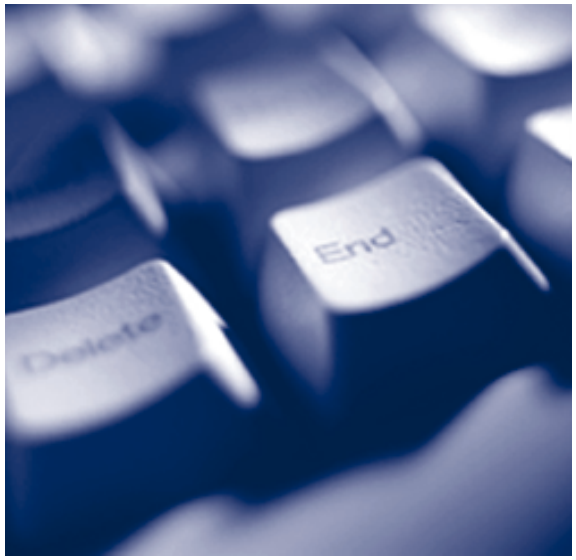
TPIPAS（臺灣個人資料保護與管理制度規範）

- 經濟部商業司也將從2013年開始，將原本只提供電子商務業者申請的驗證制度，擴大開放給經濟部商業司所主管產業的公司皆可申請，企業通過TPIPAS驗證後，則可以取得DP Mark（資料隱私保護標章）。
- TPIPAS是經濟部商業司參考日本，德國個資驗證標準所訂定的個資保護與管理制度，並依據新版個資法內容調整而成的一套個資認證制度，目前打算導入TPIPAS的企業以服務業居多。

NIST SP800-122

- 個人可識別資訊機密性保護指引
  (GUIDE TO ROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION)
- 個資防護的重要性外，並以風險為基礎，建議各項 防護措施與事故回應計畫(Incident Response Plan)。
- 文件架構：本文件共分為 5 個章節，
  - 第 1 章介紹文件的目的與範圍、使用對象及文件架構
  - 第 2 章描述何謂個資，並如何找出組織所維護的個資
  - 第 3 章說明當個資遭到不當的存取、使用及揭露時，如何決定衝擊因素
  - 第 4 章提供保護個資機密性的控制措施，以降低個資被洩漏的風險
  - 第 5 章提出如何發展個資事故回應計畫，並整合至組織現有的事故回應計劃

- 謝謝您的參與！



Turn Knowledge Into Valuable Services …