因應資安稽核：

風險管理及稽核準備

撰寫人

EY 安永

Building a better working world

安永企業管理諮詢服務股份有限公司

曾品媛
資深經理， 企業管理諮詢服務
聯絡電話：+886 2 2757 8888 ext.67814
電子郵件： Jenny.Tsen@tw.ey.com

背景介紹

- ▶ 安永企業管理諮詢服務股份有限公司經理。
- ▶ 專長於資訊安全、電腦稽核、營運持續管理及個人資料保護管理系統。
- ▶ 曾從事電腦稽核、風險管理、資訊安全管理制度及個人資料管理制度導入等相關服務。

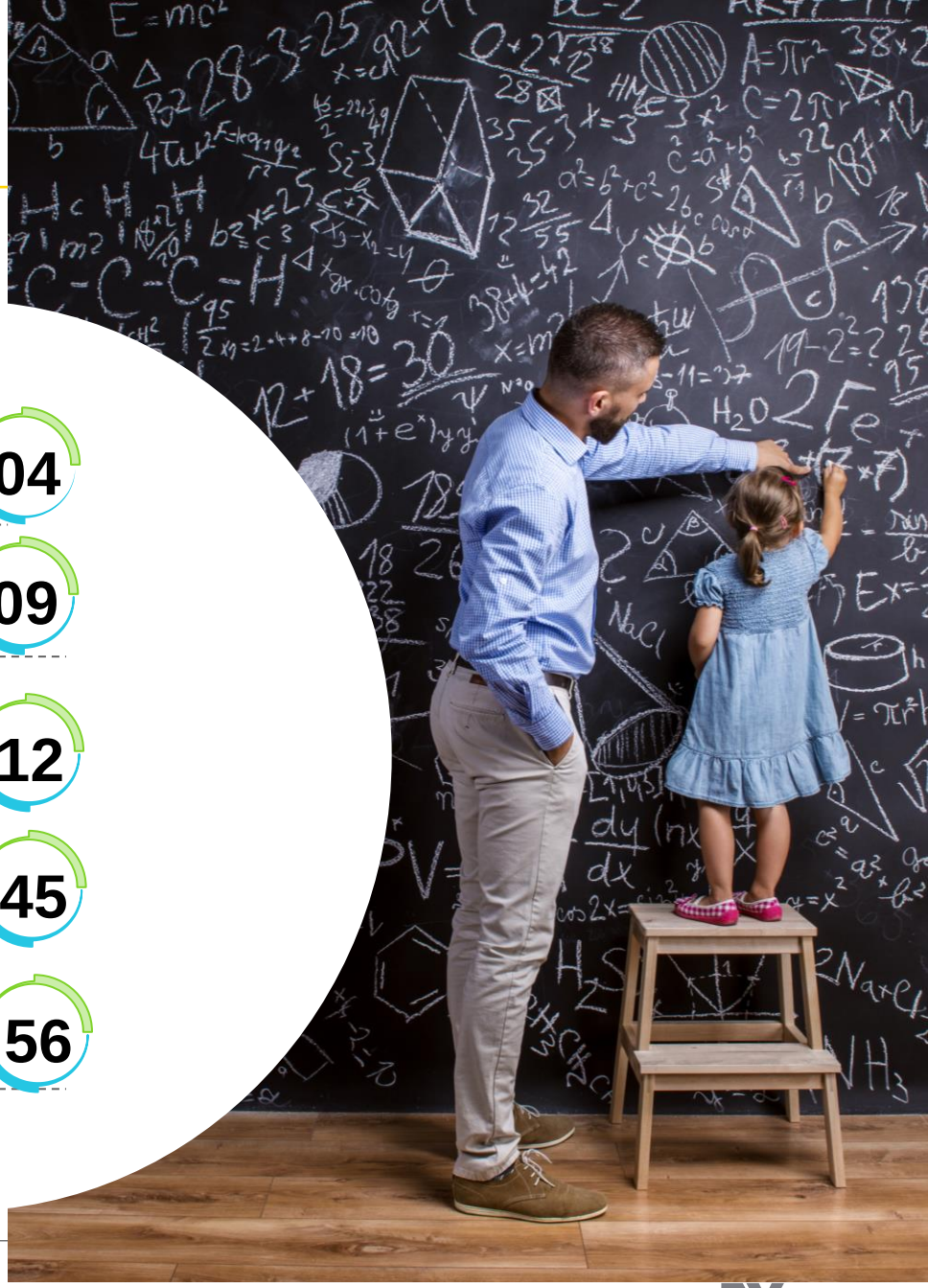
相關經驗介紹

- ▶ 擔任專案經理協助數個政府單位導入ISO 27001:2013並順利取得證書。
- ▶ 擔任專案經理協助某金融機構同時導入ISO 27001:2013 及BS10012:2009 管理制度。
- ▶ 曾協助某傳統產業評估其內控管理制度與SOX間之差異並提出改善建議。
- ▶ 擔任專案經理協助國內知名之保全業導入ISO 27001:2013 並取得證書。
- ▶ 擔任專案經理協助某外商保險公司評估其海外災害復原機制是否有符合法規要求。
- ▶ 擔任專案經理協助某IC公司執行ISO27001:2013差異分析及風險評鑑作業。
- ▶ 曾協助某外商銀行執行其供應商之資訊安全環境評估並提出改善建議。
- ▶ 曾協助某市政府資訊單位執行 資訊安全管理系統導入並順利通過 ISO 27001:2005 認證。
- ▶ 曾輔導數家大專院校執行資訊安全管理系統導入並順利取得 ISO 27001:2005 認證。
- ▶ 曾協助某政府單位執行資訊系統稽核專案，檢視內部控制制度資訊循環項目，根據相關辦法進行查核並給予建議。

學歷及專業資格

- ▶ ISO 27001:2013 LA
- ▶BS 25999 LA
- ▶國際專案管理師 PMP
- ▶國際資訊安全經理人 CISM
- ▶臺灣大學 GMBA 碩士學位
- ▶美國阿拉巴馬州立大學學士主修 Computer Science

大綱



大綱

風險概論—風險之特性

- 不確定性(Uncertainty)：
  - 事件是否會發生
  - 事件發生於何時
  - 事件發生後果之嚴重性

- 財物損失的可能性：
  - 營運中斷
  - 違反法規

- 發生於未來
  - 未知的
  - 不可預期的

風險管理概念

- 風險無所不在，藉由建立風險管理體系，在風險發生的第一時間搶得先機-降低損失或提早避免或預防

- 大部份組織面臨的最大風險
  - 不清楚如何管理風險
  - 完全不知道有風險的存在
  - 清楚有風險，確不瞭解如何去管理與執行

風險管理原則

1.設定清楚明確的目標

2.辨認可能使目標無法達成之風險

3.建立風險的控制機制

4.確認目標、風險及因應控制之一致性

風險管理效益

Identify assets 識別資產 – 我需要保護什麼?

Identify threats 識別威脅 – 我需要採取何種對策?

Calculating risks 計算風險–需要多少時間、人力、或成本來保護重要資產?

大綱

ISO 31000 風險管理流程

風險評鑑程序

資訊資產鑑別 → 資訊資產評價 → 弱點及威脅分析 → 風險值計算 → 決定可接受風險等級

風險處理程序

風險評鑑報告 → 擬訂風險處理計畫 → 執行風險處理計畫 → 評估風險處理計畫執行成效

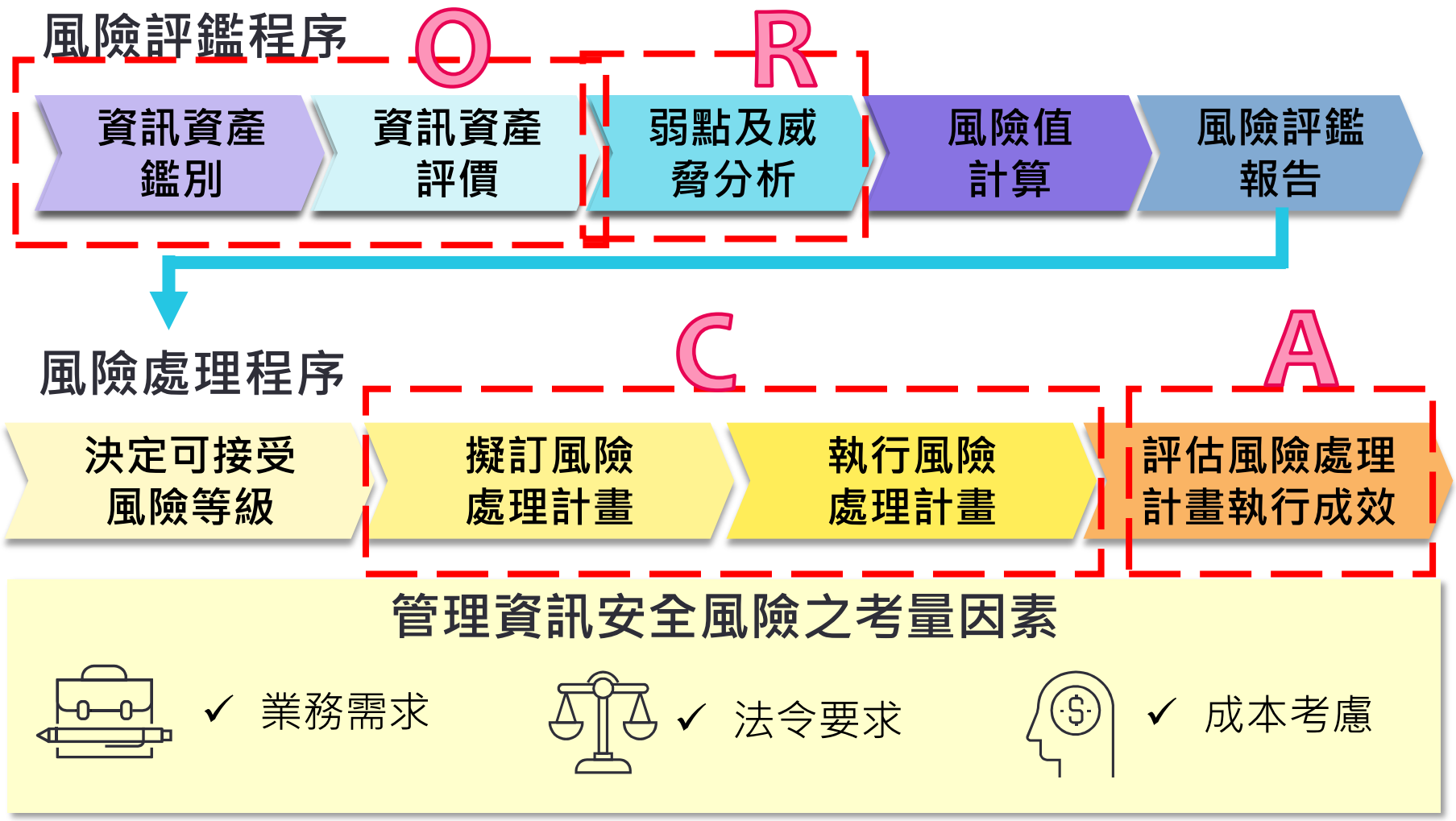
管理資訊安全風險之考量因素

✓ 業務需求

✓ 法令要求

✓ 成本考慮

ISO 31000 風險管理流程



EY安永

大綱

資訊資產辨識

何謂資訊

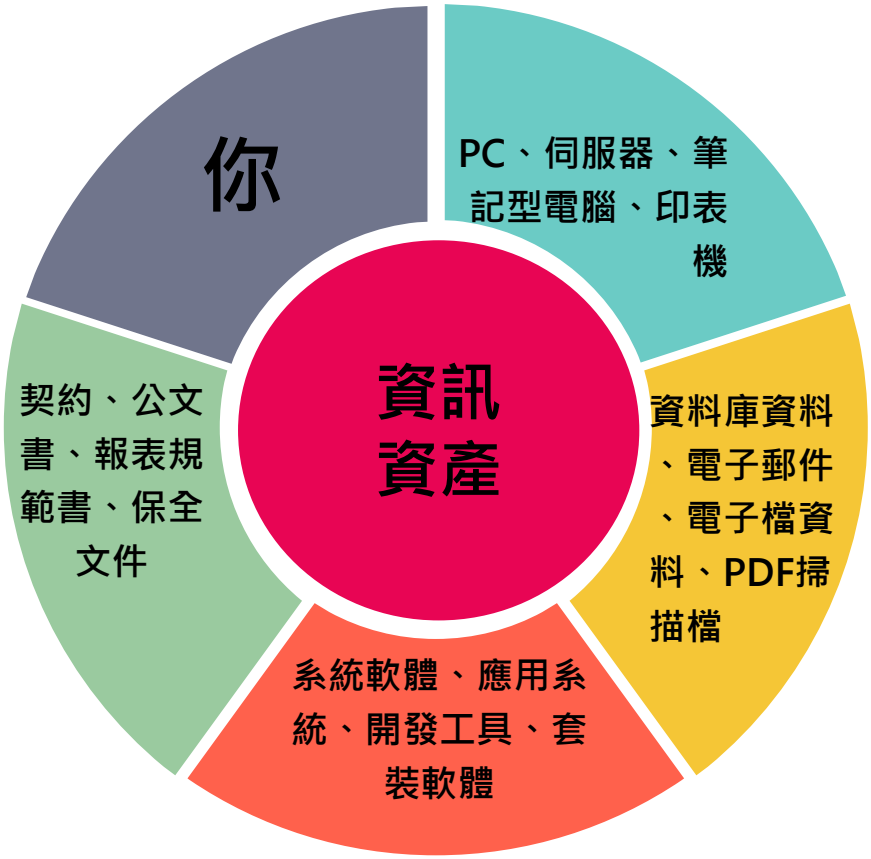

資訊
任何型態顯示及任何媒體儲存經處理過之資料
價值
資訊內容
內容
營運計畫、研究計畫、公文、員工資料合約及各項紀錄等
✓資訊是組織的重要資產

EY安永

資訊存在的形式

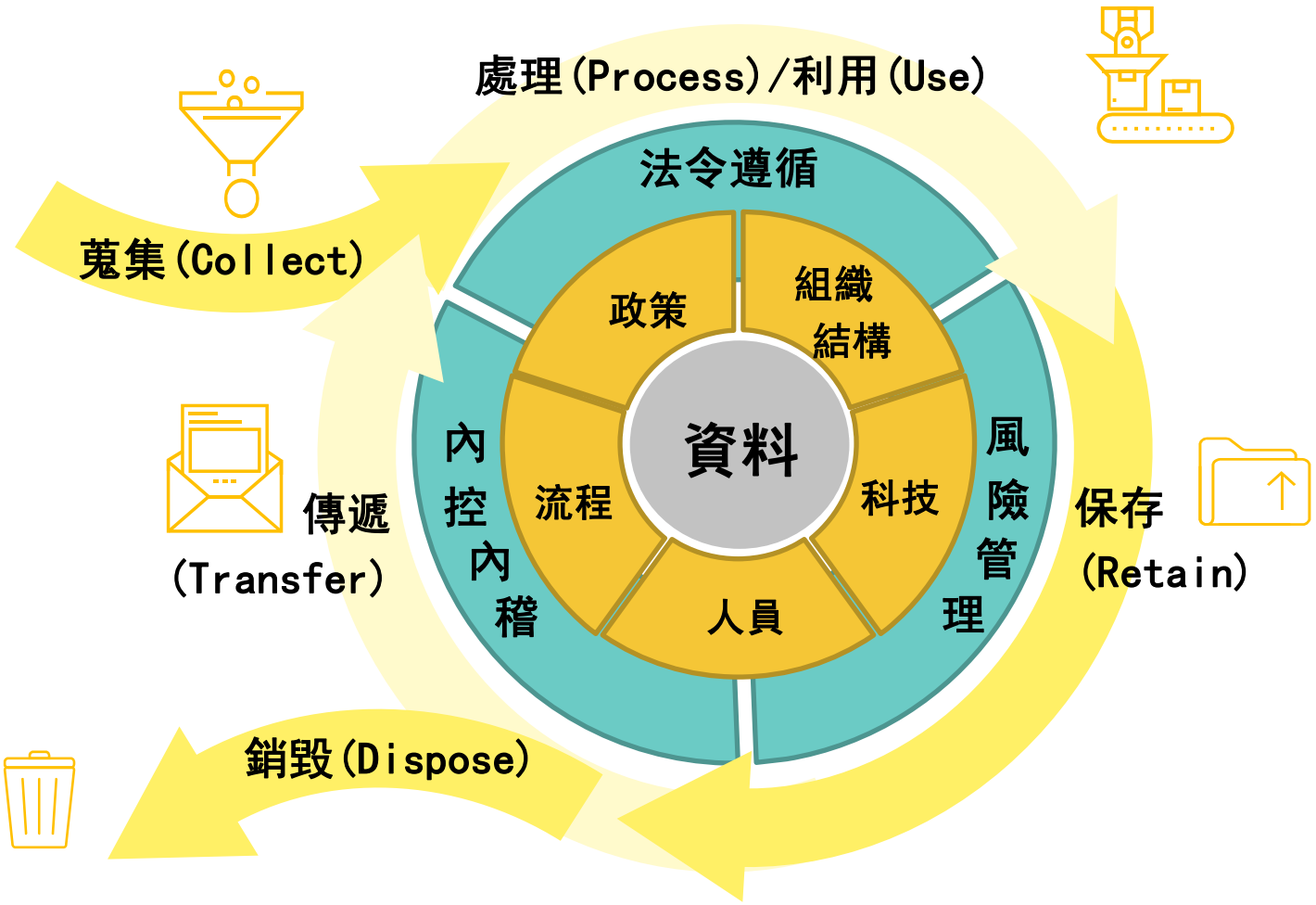
資訊產生途徑

- 列印或書寫在紙張
- 儲存於電子媒體
- 藉由郵遞或電子型態傳送
- 透過影片展示
- 正在進行的對話



『不管資訊藉由何種形式存在或共享以及儲存，它都應被適當的保護。』

資訊生命週期


處理(Process)/利用(Use)
法令遵循
蒐集(Collect)
政策
組織結構
資料
內控內稽
流程
科技
風險管理
人員
傳遞(Transfer)
保存(Retain)
銷毀(Dispose)

資訊資產

- **定義：**對組織而言有價值的資訊相關事物。
- **依業務流程**
  - 依照單位組織之業務作業流程定義其相關之資訊資產。
- **依範圍 （業務權責）**
  - 依照單位各負責人其負責之相關業務範圍辨識資訊資產。

資產盤點與分類

- 點
  - 個人工作職掌
  - 伺服器、個人電腦
- 線
  - 作業流程圖
  - 資通系統的資訊資產關連圖
- 面
  - 實體環境配置
  - 網路架構圖
  - 資產管理系統(硬體、軟體) - 財產帳

資產盤點—個人工作相關聯檢視(點)

一般硬體

個人電腦(以科為單位)

作業系統

內部人員

紙本文件

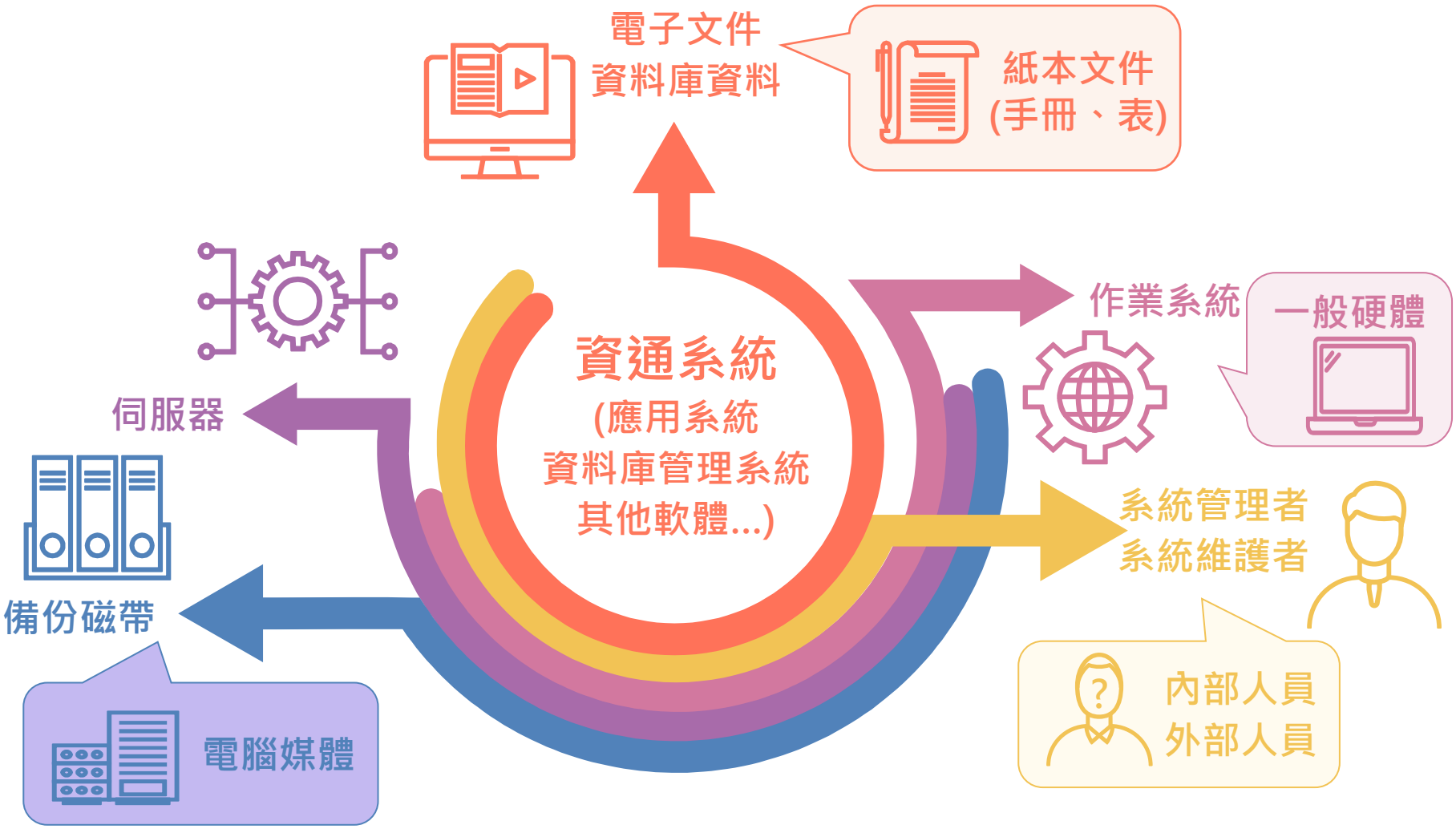
計畫、規範手冊、表單

商用軟體

商用軟體

電子文件

資產盤點—系統相資訊資產相關聯檢視(線)



EY安永

資產盤點—作業流程檢視(線)

資產分類
聯想資產

人員

文件

軟體

硬體

資料

支援設備

試問下列
問題

什麼人在做？(內、外部人員)

人員怎麼作業？(紙本、電子文件)

為什麼可以去做？(紙本、電子文件)

依據什麼辦法？(紙本、電子文件)

什麼作業原則？(紙本、電子文件)

使用什麼設備？(一般硬體)

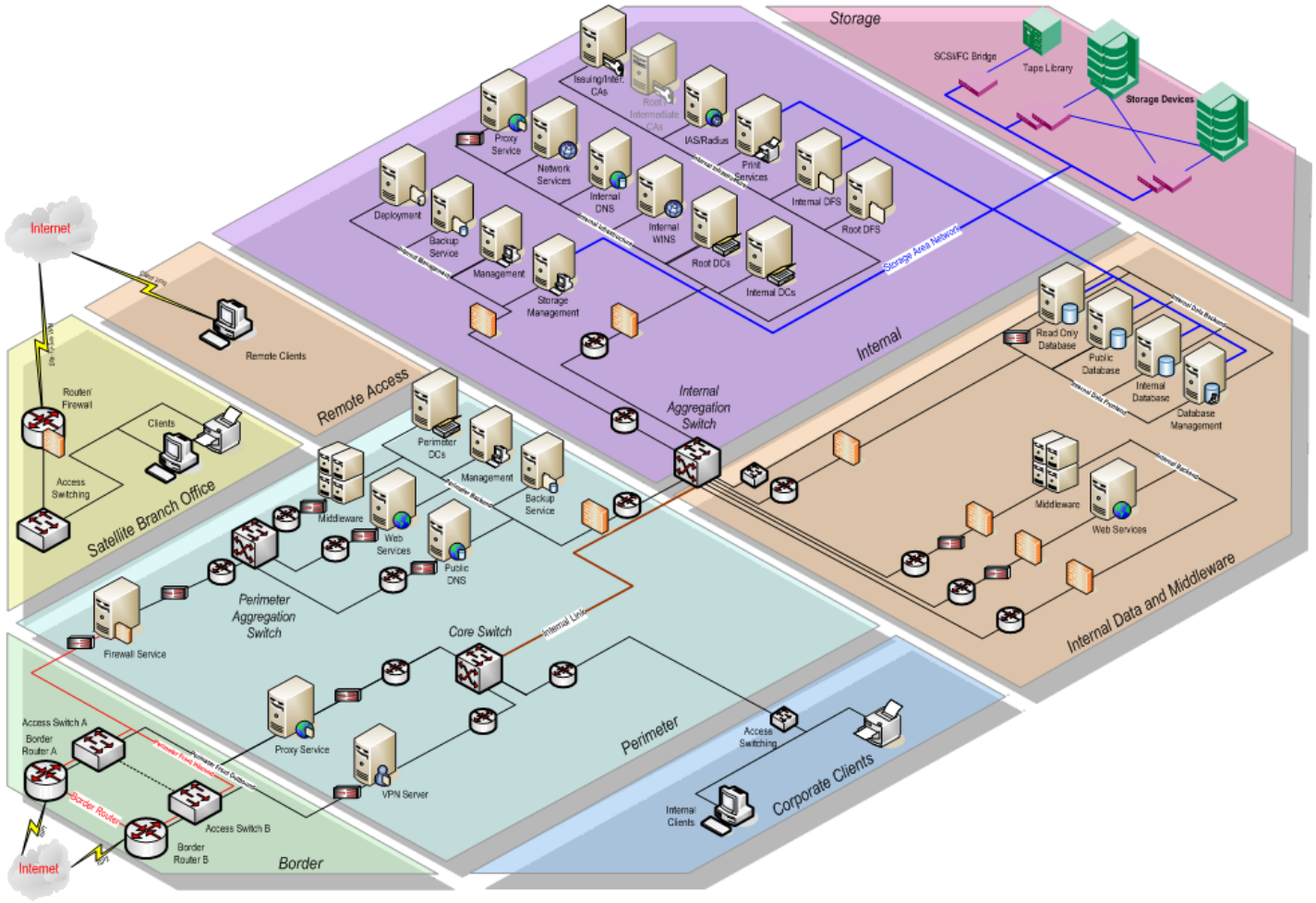
能看到或輸入什麼資料？(紙本、電子文件)

需要什麼系統與服務？(內、外部服務)

需要產出什麼資料？(紙本、電子文件)

利用什麼傳送資料或訊息？(電訊，內、外部服務)

資產盤點—網路架構檢視(面)



EY安永

資訊資產價值考量因素

- **機密性（Confidentiality）**
  - 使資訊不可用或不揭露給未經授權之個人、組織或過程的性質。
- **完整性（Integrity）**
  - 保護資產準確(accuracy)和完整(completeness)的性質。
  -
- **可用性（Availability）**
  - 經授權單位因應需求之可存取及可使用的性質。

資訊資產辨識與分級

組織花在保護資產的費用絕不應超過該資產對於組織的價值。

資訊資產分級之目地為

- ✓ 為防護措施提供一個可遵循之依據

- ✓ 鑑別資產之敏感性及其重要性

- ✓ 確保資產依據重要等級給予相對應之保護措施

- ✓ 協助制定有效的風險管理計劃

資訊資產類別(一)

- **軟體（ Software ）：**
  - 應用系統、系統軟體、開發工具、套裝軟體及公用程式等。
- **硬體（ Hardware ）：**
  - 網路設備、主機設備、Notebook及傳真機等。
- **資料（ Data ）：**
  - 數位資訊、交易資料及資料檔等。
- **文件（ Paper Documents ）：**
  - 契約、公文書、報表、規範書、計畫書及發票等。

資訊資產類別(二)

- **通訊（ Communication ）：**
  - 網路及語音服務等。
- **環境（ Environment ）：**
  - 電、水、照明、空調等。
- **人員（ People ）：**
  - 員工、約聘僱人員及委外人員（如：委外維護工程師、清潔人員）等。

資訊資產分類說明(一)

代碼	母類別	子類別	舉例
1	資料	電子文件	儲存於硬碟、磁帶、光碟等儲存媒體之數位資訊，如交易資料、連線主檔、資料庫資料檔等
2	文件	紙本文件	以紙本形式存在之文書資料、報表等相關文件，如契約、公文書、列印之報表、表單、計畫、規範書、計劃書及發票等
3	軟體	商用軟體	系統軟體、套裝軟體等
		內部開發軟體	開發工具、自行開發及委外開發之應用系統，如原始程式碼、應用程式執行碼、資料庫系統等
4	硬體	一般硬體	硬碟、磁帶、光碟、網路設備(如路由器、交換器、集線器)、主機設備、電腦工作站、筆記型電腦、影印機、印表機、傳真機等

資訊資產分類說明(二)

代碼	母類別	子類別	舉例
5	人員	內部人員	員工、約聘僱人員
		外部人員	廠商委派支援本單位之第三方人員（含常駐與非常駐人員），如廠商維護工程師、清潔人員、保全人員等
6	通訊	外部服務	提供資訊傳輸、交換之線路或服務，如專線（資料及語音傳輸之線路）、網際網路等
7	環境	環境	建築物，如辦公室、機房；以及相關基本設施，如水電、消防、照明、空調等

資訊資產相關人員

- **資訊資產擁有者(權責單位)**
  - 具資訊資產之所有權，負責資訊資產之平日安全管理責任 。
- **資訊資產管理者(保管單位)**
  - 由資訊資產擁有者授權取得管理之責，負責落實受委託保管資訊資產 。
- **資訊資產使用者(使用單位)**
  - 從資訊資產管理者取得資訊資產之使用權，因業務需求，會直接或間接使用到該資訊資產之單位 。

資訊資產相關責任

- **資訊資產擁有者(權責單位)**
  - 規劃資訊資產分類與分級辦法，鑑別及評價其所管轄內之所有資訊資產，並指派資訊資產管理者。
- **資訊資產管理者(保管單位)**
  - 對保管之資訊資產協助資訊資產擁有者進行資產評價、維護管理，並規劃及執行適當的控制措施。
- **資訊資產使用者(使用單位)**
  - 對於被授權使用資訊資產之人員或單位，應依各項安全程序，正確使用及操作。
- **單位主管**
  - 負責指派專人維護資訊資產清冊。
  - 負責監督資訊資產分類、分級執行與管理。

風險辨識

風險是?

- 發生可能會影響目標達成的事件
  - 目標 = 準時抵達公司
  - 流程 = 起床、著衣、吃早餐、出門、搭車、到達公司
  - 事件 = 賴床、鬧鐘壞掉、塞車、門壞掉、汽車拋錨
  - 事件發生的機率 = ? (高、 中、 低)
  - 事件造成的衝擊 = ? (高、 中、 低)

辨識弱點

- **弱點(Vulnerability):**
  - 是指組織資訊安全的弱點或漏洞，本身不會造成傷害，但若未妥善管理，則可能造成威脅的得逞。
- **辨識方法**

- 確認資產之安全弱點

—是否有安全問題
—是否有遺漏之安全控管措施
—目前保護機制，是否有弱點

- 確認作業環境之安全弱點

—應用技術
—網路連線
—實體安全
—人員教育訓練
—資訊安全意識
—是否遵守相關規定等

辨識威脅

- 定義
  - 可能會對系統或組織及其資訊資產造成傷害的事件，資產通常都會面臨許多不同的威脅：**威脅必須利用資產的弱點才能對資產造成傷害**

天然災害：颱風、地震、水災及停電等

地震可能威脅到資訊資產的可用性及完整性

辨識威脅

人為因素：非法存取資料、偷竊及竄改資料等

偷竊可能威脅到資訊資產的可用性及機密性

辨識威脅

技術因素：服務失效及硬體故障等

硬體故障可能威脅到資訊資產的機密性、可用性及完整性

風險評鑑

弱點容易被利用之程度(脆弱度)

弱點評估標準	容易被利用	等級
資訊資產控管強度高，非常不容易被威脅利用。	低	1
資訊資產控管強度中，較容易被威脅利用。	中	2
資訊資產控管強度低，非常容易被威脅利用。	高	3

威脅發生之可能性

威脅發生可能性評估標準	機率	等級
發生機率低：一年發生小於1次。	低	1
發生機率中：一年發生超過1次（含），小於4次。	中	2
發生機率極高：一年超過4次（含）。	高	3

風險計算公式

資產價值 = 機密性、完整性、可用性，取最大值。

風險之定義與評估

風險值=資產價值 * 威脅等級 * 弱點等級

風險值對照表

資產價值	威脅可能性	弱點容易被利用程度		
		低(1)	中(2)	高(3)
1	低(1)	1	2	3
	中(2)	2	4	6
	高(3)	3	6	9
2	低(1)	2	4	6
	中(2)	4	8	12
	高(3)	6	12	18
3	低(1)	3	6	9
	中(2)	6	12	18
	高(3)	9	18	27
4	低(1)	4	8	12
	中(2)	8	16	24
	高(3)	12	24	36

威脅、弱點、風險之間的關係(例)

- 小陳居住在美國布魯克林區的老舊公寓一樓，出門並沒有將門上鎖的習慣, 家裡的珠寶、美金並未放置保險箱內。

- 資產= 珠寶、美金
- 威脅= 小偷光顧
- 弱點= 沒有上鎖的習慣
- 風險(風險情境)= 遭小偷財產損失
- 影響= 生活、家庭....

風險情境發生可能性= 威脅*弱點

威脅、弱點、風險之間的關係(例)

- ABC壽險公司內部同仁資安意識薄弱，經常點選外部郵件導致電腦經常中毒，近日常有駭客透過電子郵件社交工程植入惡意程式以竊取保戶資料，

  - 資產= 保戶資料
  - 威脅= 駭客攻擊
  - 弱點= 資安危機意識不足
  - 風險(風險情境)= 保戶資料外洩
  - 影響=公司聲譽 財務損失

風險情境發生可能性= 威脅*弱點

評估結果檢查與確認

- 組織重要資產是否有被凸顯？
- 作業或流程重要資產是否有被凸顯？
- 機密性極高是否有被凸顯？
- 完整性極高是否有被凸顯？
- 可用性極高是否有被凸顯？
- 風險值極高？
- 風險值極低？

是否合理、可以解釋？

大綱

風險管理策略與方法

策略：

方法：

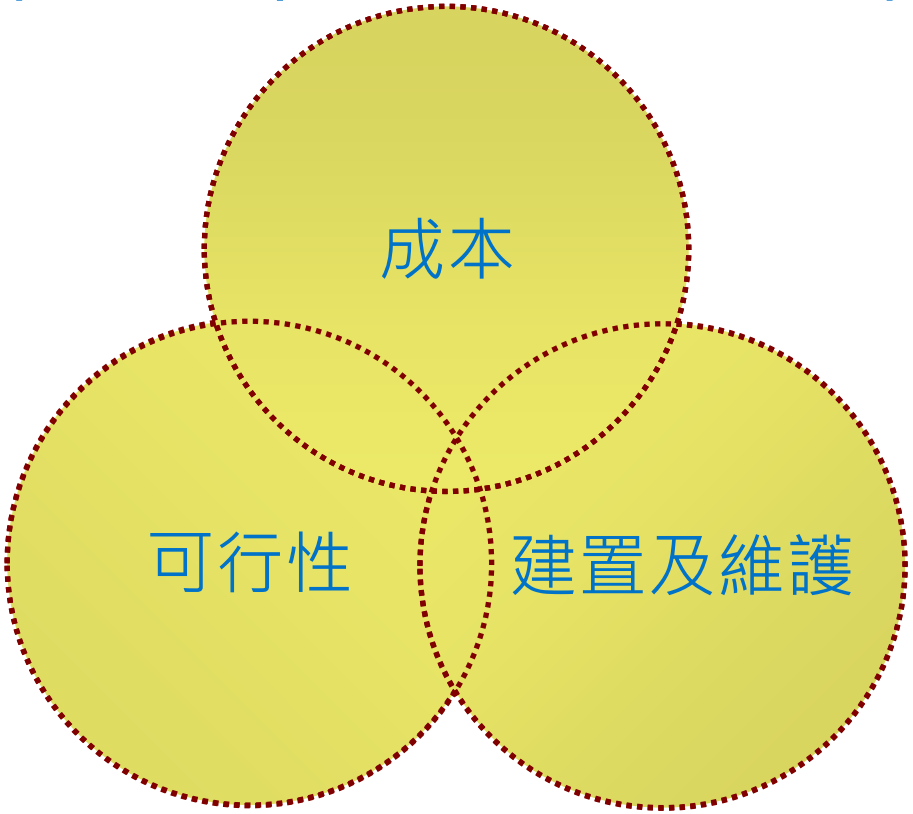
- 減少威脅發生機率
- 強化弱點防護
- 改變作業方式
- 分散風險損失
- 降低資產價值

風險管理要素

- 可接受風險值（Risk Acceptance）：範圍內各類資訊資產之最低風險容忍度
- 現有控管：範圍內各類資訊資產目前之控管措施
- 殘餘風險：範圍內各類資訊資產在採用相關控制措施之後剩餘的風險

風險處理考量原則

(More expensive than assets)



(Difficult or Impossible)

(Time and Cost)

風險處理考量範例

- 安全風險所造成之影響
- 需要的安全保證等級
- 所需費用及時間是否合理
- 技術上是否可行
- 是否能與作業環境配合
- 符合法令規定
- 相關契約規定

風險處理--選擇控制措施

預防型	偵測型	修正型	回復型	指示型
• 密碼管理	• CCTV監控	• 定期上Patch	• 金鑰回復	• 操作手冊
• 權限管控	• 入侵偵測	• 災害復原計畫	• 備份還原	• 資安政策
• 門禁管控	• 病毒偵測		• 檔案修復	• 告示牌

風險處理計劃--可接受風險值

- 可接受風險值應考量組織環境及作業之安全需求作適當調整
- 資訊資產之可接受風險值，需經資訊安全組織開會決議，並記載於會議紀錄中
- 定期召開會議檢討可接受風險值

風險處理計劃--殘餘風險

- 殘餘風險（Residual Risk）
- 是可接受風險與未識別風險之總和
- 應取得管理階層對各項可接受風險的核准
- 依已規劃的期間，審查風險評鑑結果，並審查殘餘風險的等級及已識別的可接受風險，並將下列事項之變更納入考量：
  - 組織
  - 技術
  - 各項營運目標與過程
  - 已識別的威脅

風險處理計劃

- 範圍：針對超出可接受風險值之資訊資產
- 目標：有效管理風險
- 方法：選擇適當之控管措施，說明風險控管措施之執行辦法，並列入追蹤管理程序

- 要項：
  - 資訊資產
  - 權責單位
  - 現況說明
  - 風險改善措施
  - 風險改善時間

風險管控措施之執行及追蹤

- 控管措施監督：

  風險改善計畫之執行，應彙整控管，並設立持續追蹤機制。

- 控管有效性：

  於各風險改善措施完成後，進行風險再評估，以確保相關改善措施的有效性。

結語

- 風險管理並無法確保100%的無風險。
- 「威脅/脆弱之所在 風險之所在」，透過系統化的方法(風險評鑑管理程序)，找出風險所在，已適時選擇控制措施加以處理。
- 持續性之風險管理，在於確保組織資訊資產均處於最佳保護之下 。

大綱

資通安全管理法施行細則

行政院　民國110年8月23日　院臺護字第1100182012號

修正「資通安全管理法施行細則」第6條、第7條、第13條條文、「資通安全責任等級分級辦法」第5條、第6條、第7條條文及第11條附表1至附表8、附表10、「資通安全事件通報及應變辦法」第6條、第13條、第21條條文、「特定非公務機關資通安全維護計畫實施情形稽核辦法」第3條、第6條、第10條條文、「資通安全情資分享辦法」第3條、第11條條文及「公務機關所屬人員資通安全事項獎懲辦法」第4條、第7條條文

資通安全威脅偵測管理機制
初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心

備註二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證 之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。

稽核常見問題

- ✓ 是否設置資通系統之備援設備，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？(資通系統等級中/高等級者適用)
- ✓ 是否規劃及執行稽核發現事項改善措施，且定期追蹤改善情形？
- ✓ 是否建立資通安全情資之評估及因應機制，針對所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施？
- ✓ 是否適時進行資通安全情資分享？分享哪些資訊？
- ✓ 是否訂定電子郵件之使用規則，且落實執行？是否依郵件內容之機密性、敏感性規範傳送限制？
- ✓ 是否針對資通系統及相關設備，建立適當之監控措施(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)？是否針對日誌建立適當之保護機制，以避免遭到竄改，且落實執行並定期稽核？

稽核常見問題-委外廠商(1)

- ✓ 是否訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，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**或**通過第三方驗證**？
- ✓ 是否皆已指定專案管理人員，負責推動、協調及督導委外作業之資通安全管理事項？
- ✓ 是否配置充足且經適當之資格訓練、擁有**資通安全專業證照**或**具有類似業務經驗**之資通安全專業人員？
- ✓ 是否針對**委外業務項目進行風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？

稽核常見問題-委外廠商(2)

- ✓ 是否依委外業務項目之性質允許委外廠商就委外業務項目分(轉)包？如允許分(轉)包，是否注意分(轉)包之範圍，以及分(轉)包之廠商是否具備資通安全維護措施？
- ✓ 是否依資通系統分級，於徵求建議書文件(RFP)相關採購文件中明確規範防護基準需求？
- ✓ 對於核心資通系統之委外廠商，是否針對其人員(如能力、背景等)及開發維運環境之資通安全管理進行評估？
- ✓ 委外客製化資通系統開發者，是否要求委外廠商提供資通系統之安全性檢測證明，並針對非委外廠商自行開發之系統或資源，標示非自行開發之內容與其來源及提供授權證明？若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，是否自行或另行委託第三方進行安全性檢測之複測？

稽核常見問題-委外廠商(3)

- ✓ 是否訂定委外廠商對於機關委外業務之資安事件通報及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，是否立即通知機關並採行補救措施？
- ✓ 委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料？
- ✓ 是否定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務、報告及紀錄等進行管理及安全檢視(如廠商端實地稽核、要求廠商提供異常報告、要求廠商提供相關安全檢測紀錄等)，以利後續追蹤及管理？

稽核常見問題-系統開發(1)

- ✓ 針對自行或委外開發之資通系統是否依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施？
- ✓ 資通系統開發過程請是否依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求？
- ✓ 資通系統開發前，是否設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形？
- ✓ 資通系統設計階段，是否依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估？
- ✓ 資通系統開發階段，是否避免常見漏洞(如OWASP Top 10等)？且針對防護需求等級高者，執行源碼掃描安全檢測？

稽核常見問題-系統開發(2)

- ✓ 資通系統開發階段，是否避免常見漏洞(如OWASP Top 10等)？且針對防護需求等級高者，執行源碼掃描安全檢測？
- ✓ 資通系統上線前，是否執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試等，且檢討執行情形？
- ✓ 資通系統開發如委外辦理，是否將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約？
- ✓ 是否將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安保護措施？

稽核之整備事項

安全維護計畫整備事項

- ✓ 更新資安專責人員分工表、個人資料保護管理執行小組名單、個人資料保護管理專人名冊、個人資料保護管理執行小組稽核專人名單、資通安全專責人員分工表。
- ✓ 安全維護計畫實施情形提報之佐證資料。
- ✓ 安全維護計畫實施情形填報內容與實務狀況是否有遺漏或不一致之情形，應確實檢核提報資料之正確性。

稽核之整備事項

資安法及施行細則

- ✓ 新案的RFP配合調整：業務委外之廠商資格或評選項目加入「資安法施行細則第四條」之要求。
- ✓ 修改RFP範本、契約範本（應將監督受託者資通安全維護情形放入契約中要求廠商）：
  1. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
  2. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
  3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
  4. 受託者應採取之其他資通安全相關維護措施。
  5. 應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

稽核之整備事項

資安法及施行細則

- ✓ 委外廠商遴選，應確保受託廠商具備完善之資通安全管理措施或通過第三方驗證及執行人員應具有資通安全專業證照或類似之資通安全專業人員。辦理遴選作業時，應針對計畫團隊相關人員之資通安全專業能力要求，進行相關評估作業。

稽核之整備事項

資通安全責任等級分級辦法

- ✓ 全部核心資通系統導入CNS 27001 或ISO27001 等資訊安全管理系統標準，並於三年內完成公正第三方驗證，並持續維持其驗證有效性。
- ✓ 配置2名資通安全專責人員，且均有資通安全專業證照、資通安全職能評量證書，並符合每年規定之教育訓練時數。
- ✓ 每2年辦理1次全部核心系統進行業務持續運作演練
- ✓ 每年辦理1次內部資通安全稽核
- ✓ 每年1次資安治理成熟度評估：上傳紀錄
- ~~✓ 限制使用危害國家資通安全產品：是否於已汰除危害資安之設備，如有特殊因素請列冊列管。~~

稽核之整備事項

資通安全責任等級分級辦法

- ✓ 全部核心資通系統每年辦理二次網站安全弱點檢測
- ✓ 全部核心資通系統每年辦理一次系統滲透測試
- ✓ 每年辦理一次資通安全健診，含括網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視
- ✓ 完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。含括防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制、入侵偵測及防禦機制、具有對外服務之核心資通系統者，應備應用程式防火牆、進階持續性威脅攻擊防禦措施。

稽核之整備事項

資通安全責任等級分級辦法

- ✓ 部內所有資訊系統均完成資通系統分級，每年至少檢視一次資通系統分級妥適性。
- ✓ 部內所有自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施。
- ✓ 防護基準符合之佐證。

資通安全情資分享辦法整備事項

- ✓ 是否依資通安全情資分享辦法建立資通安全情資評估及因應機制。

稽核之整備事項

其他整備事項

- ✓ 所有資訊系統均需進行資訊資產盤點，並填寫資訊資產清冊。
- ✓ 是否已將物聯網設備納入資訊資產盤點範圍，並建立適當防護措施。
- ✓ 委外合約：系統開發生命週期各階段依等級將資安需求(含機密性、完整性、可用性)納入委外合約
- ✓ 確認已就 GCB 套用之例外管理，提出可行方式及改善時程，並定期追蹤改善情形。
- ✓ 是否要求委外廠商限制使用危害國家資通安全產品。

Q & A