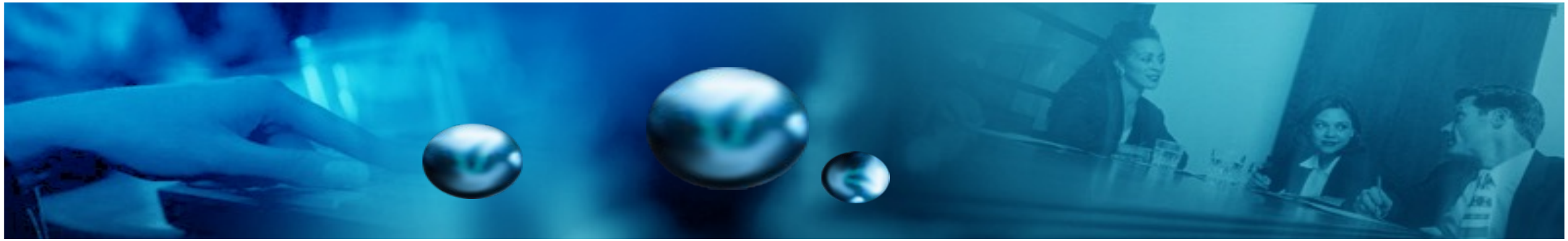
資訊資產管理概論與實務



輔導顧問師 曾立民

Mobile: 0980-292282

E-mail: linklong685@gmail.com

SafeLink 博創資訊科技股份有限公司

目錄

01 概論

知識資產變成文件資料後文件資料量爆炸、一旦發生錯誤又要更改管理耗費人力物力。.

02 條文要求

所有重要資訊的資產應被制定並維護，紀錄詳細資訊如：
型式 (例如：軟體、物質的/印刷的、服務、人、無形資產)

03 實務做法

組織應明訂與適用一個資訊安全處理過程，以：c) 比較在上述6.1.3 b)決定的管制與附錄A的，且確認沒有忽略到必要的管制.

04 結論

資訊資產做的好，要靠以下四大類IT應用：外部資料電子化：允許工具形式有哪些內部文件無紙化：表現內部文件的工具
.

概論

資產

對組織具有潛在或實際價值的項目，事物或實體

資產管理是一門建立完善的機制，定義一個由相互關聯和相互作用的部分組成的系統，以建立政策，目標，策略，計劃和活動
在指定的責任期限內，通過資產組合實現組織目標的最大化績效和價值。 在這種情況下，“部分”包括業務流程和治理活動，“績效”包括運營，財務和法律績效，“價值”包括成本和風險的最小化。

資產管理
協調組織活動，以從
資產中實現價值.

價值

價值可以是有形的或無形的，財務的或非財務的，並且包括對風險和負債的考慮。 在資產壽命的不同階段，它可以是正數或負數。

實體資產

實體資產通常是指組織擁有的設備，庫存和財產。.

無形資產

有形資產與無形資產相反，無形資產是非有形資產，例如租賃，品牌，數字資產，使用權，許可，知識產權，聲譽或協議。

資產分類

稱為資產系統的資產分類也可以視為資產.

基本概念

資產管理 IT資產管理（ITAM）和軟體資產管理（SAM）

資產管理應用於資產生命週期的每個階段。在許多行業中，資產管理在確定組織的運營績效和效率方面起著關鍵作用。

ITAM

資訊技術（IT）資產管理（ITAM）是資產管理的一個分類，專門用於管理IT資產及其組成的基礎結構的生命週期和總成本。 ITAM對於支持IT環境的生命週期管理和策略決策至關重要，並結合了特定方法來處理某些類型的IT資產（例如筆記型電腦和智慧手機）的可攜性。

SAM

軟體資產管理（SAM）是另一個分類，專門用於管理軟體資產的獲取，發布，部署，維護和最終報廢。 SAM流程可對組織內的軟體資產進行有效的管理，控制和保護。 SAM結合了特定的方法來應對SAM特有的挑戰，例如分佈式和虛擬化環境中軟件資產的實時移動性，這種移動性導致軟件資產數量和多樣性的不受管理的增長。.

ALL

大多數實際情況下，兩者(ITAM, SAM)的範圍是相同的，因為SAM要求在其範圍內包括使用或管理範圍內的軟體所必需的所有其他相關資產。實際上，這意味著用於部署，執行和管理軟體的所有IT硬體資產都必須包含在SAM的範圍內。

軟體資產管理(直接益處)

Option A

通過減少IT問題來提高人員激勵和客戶滿意度

Option B

有效地向組織部署軟件以支持實現業務目標能夠更快地處理業務收購，合併或分立的IT方面

Option C

能夠響應市場機會或需求，更快，更可靠地部署新系統和功能

Option D

由於更完整，更透明的資訊可用性，因此可以做出更好的品質決策（例如，IT採購和系統開發決策可以做得更多）

Option E

提供更符合業務需求的IT，從而確保所有用戶都可以訪問適當的軟體和應用程序

Option F

更高品質的IT策略，可基於現代架構（例如，基於雲的服務和私有雲彈性

軟體資產管理

降低了軟體和相關資產的直接成本，例如通過改進使用批量合同安排的方式進行更好的定價談判，以及在可以重新分配Id的許可證時避免購買新的許可證；

通過確保所需的流程高效和有效，降低了用於管理軟件和相關資產的基礎架構成本

由於可獲得更好的信息，減少了與供應商談判的時間和成本

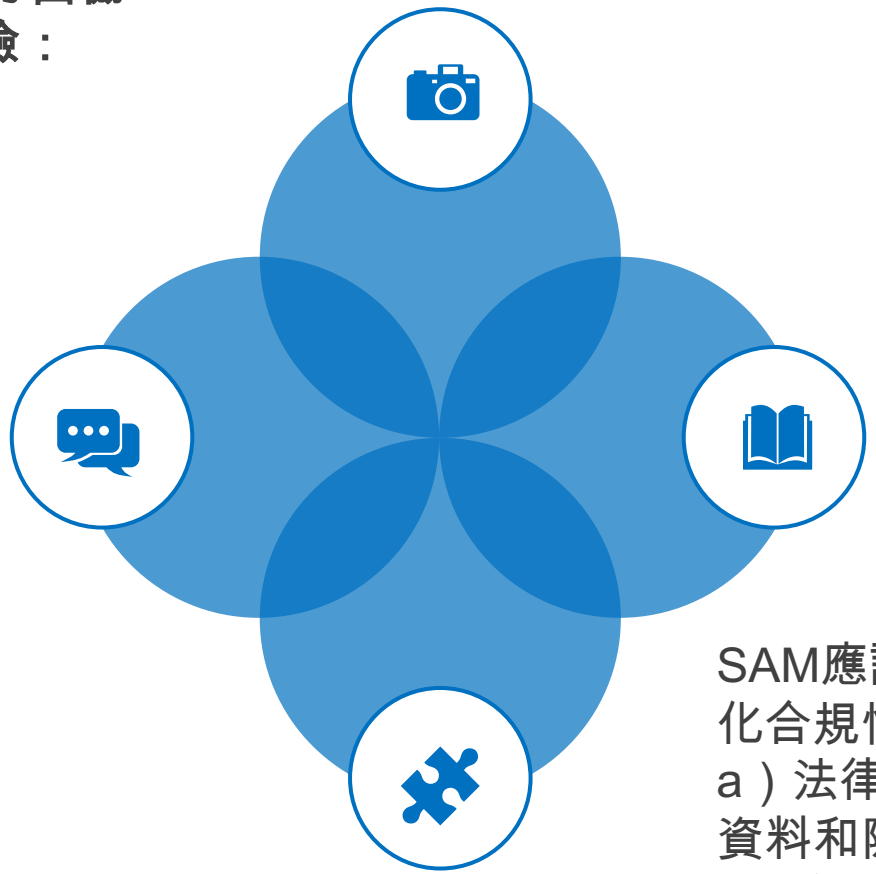
降低了支持成本，這直接受到SAM流程質量的直接影響，既直接在IT內部，也間接在最終用戶區域內

通過改善財務控制，例如更好的發票對賬以及更準確的預測和預算，來降低成本

使用IT基礎架構更好地識別會導致高成本的組件

軟體資產管理(風險)

SAM應在以下幾個方面協助管理和控制輕風險：
a) 可操作的
b) 安全性
c) 合規性



安全性風險管理和控制

SAM應該通過以下方式幫助管理和增強安全性：
a) 對已安裝和/或使用的軟件的授權有更高的證明；
b) 更好地識別未經授權的軟體； 和
c) 嚴格控制已安裝軟體的修補過程

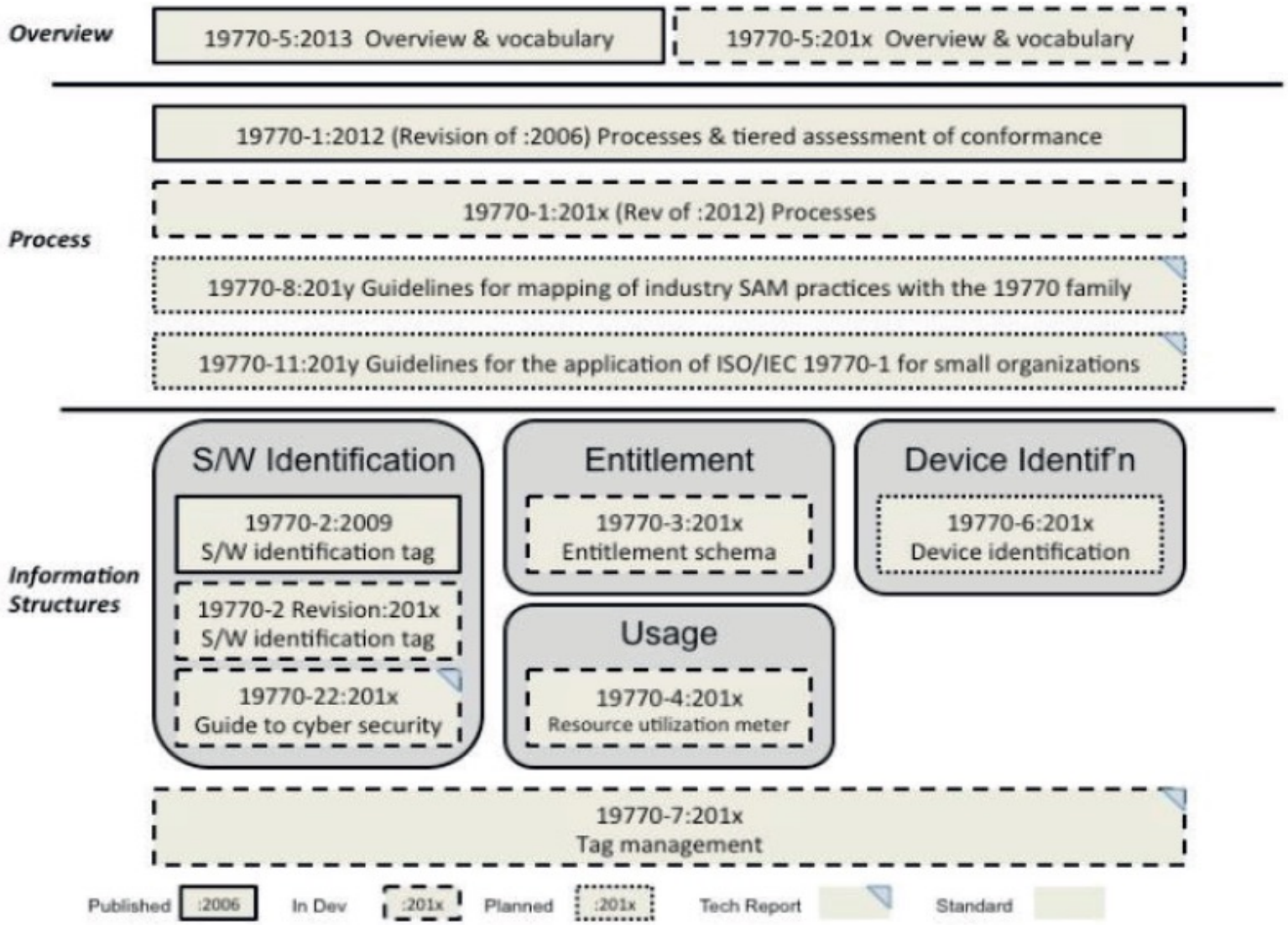
操作風險管理和控制

SAM應促進業務風險的管理，包括：
a) 中斷IT服務的風險； 和
b) IT服務品質降低的風險.

合規性作風險管理和控制

SAM應該通過最小化以下內容來促進並簡化合規性管理：
a) 法律和法規方面的風險，特別是在個人資料和隱私方面；
b) 違反許可規定；
c) 不遵守政策； 和
d) 以上任何一種行為均可能損害公共形象。

ISO 19700系列


Overview
19770-5:2013 Overview & vocabulary
19770-5:201x Overview & vocabulary
19770-1:2012 (Revision of :2006) Processes & tiered assessment of conformance
Process
19770-1:201x (Rev of :2012) Processes
19770-8:201y Guidelines for mapping of industry SAM practices with the 19770 family
19770-11:201y Guidelines for the application of ISO/IEC 19770-1 for small organizations
Information Structures
S/W Identification
19770-2:2009 S/W identification tag
19770-2 Revision:201x S/W identification tag
19770-22:201x Guide to cyber security
Entitlement
19770-3:201x Entitlement schema
Usage
19770-4:201x Resource utilization meter
Device Identif'n
19770-6:201x Device identification
19770-7:201x Tag management
Published :2006
In Dev :201x
Planned :201x
Tech Report
Standard

ISO 27001條文要求

6.1.2資訊安全風險評鑑

c)識別資訊安全風險
1)適用的資訊安全評鑑過程，以識別與ISMS範圍內之資訊機密性、完整性與可用性損害有關之風險；

7.5.3文件化資訊的管制

ISMS與本標準必需的文件化資訊應受管制以確保

A.8.2 資訊分類

A.8.2.1資訊分類
A.8.2.2資訊標示
A.8.2.3資產處置

第六章	第七章7.1	第七章7.5	A.8.1 資產責任	A.8.2 資訊分類	A.8.3 媒體的處置

7.1資源

組織應決定與提供用來建立、實施、維護和持續改進ISMS所需的資源。

A.8.1 資產責任

A.8.1.1資產清冊
A.8.1.2資產的擁有權
A.8.1.3資產之可被接受的使用
A.8.1.4資產歸還

A.8.3 媒體的處置

A.8.3.1可攜式媒體的管理
A.8.3.2媒體的處理
A.8.3.3實體媒體的傳送

實務做法

START

業務流程

藉由資通系統所提供的業務流程活動，識別該資通系統之資訊及資通系統資產.

資產分類

思考業務流程中輸出/入所代表的相關資產，並依照分類規則執行分類

資產價值

依據資產之機密性、可用性及完整性評定相關資產價值.

執行管理

依照所評定之資產價值執行保護及相關管理措施，並定期更新資產清冊

業務流程

輸入

❖資源
❖負責人
❖變更

❖文件
❖紀錄
❖表單

輸出

❖衡量標準
❖報告

核心系統(施行細則)

第七條 前條第一項第一款所定核心業務，其範圍如下：
一、公務機關依其組織法規，足認該業務為機關核 心權責所在。
二、公營事業及政府捐助之財團法人之主要服務或 功能。
三、各機關維運、提供關鍵基礎設施所必要之業務。
四、各機關依資通安全責任等級分級辦法第四條第 一款至第五款或第五條第一款至第四款涉及之 業務。
前條第一項第六款所稱核心資通系統，指支持核心 業務持續運作必要之系統，或依資通安全責任等級分級 辦法附表九資通系統防護需求分級原則之規定，判定其 防護需求等級為高者。

資訊系統(核心)

核心業務	核心資通系統	重要性說明	業務失效影響說明	RTO
		□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級A 級或B 級機關所涉業務 □為本機關依組織法執掌，足認 為重要者	財務損失： 民眾生命財產損失： 經濟發展受阻： 影響其他機關業務運作 (相依性)： 違反法遵義務： 機關信譽： 其他：	
全國公務人員人事管理 (範例)	全國公務人員人事管理系統	□為主管機關指定之關鍵基礎設施 為主管機關核定資通安全責 等級A 級或B 級機關所涉業務 □為本機關依組織法執掌，足認為重要者	違反法遵義務:依個人資料保護法應善盡個人資 料保護責任，如違反該法致足生損害他人者將受罰。	4小時

資訊系統(非核心)

非核心業務	業務失效影響說明	最大可容忍中斷時間
公文交換 (範例)	電子公文無法即時送達機關，影響 機關行政效率	〇小時
其他-非屬上開業務範疇及核心業務者(範例)	影響機關行政效率	〇小時

各欄位定義：

1. 業務名稱：公務機關之非核心業務至少應包含輔助單位之業務 名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際 情形列出)
2. 業務失效影響說明：說明該業務失效時之影響。
3. 最大可容忍中斷時間單位以小時計。

安全等級評估表

「停車管理系統(參考範例)」安全等級評估表

功能說明：提供停車場所查詢，以及汽機車未繳費資料查詢線上服務。

業務屬性：□行政類■業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	高	普	中	高
		資訊系統安全等級：		高

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，資料保護不當，將遭受一定程度之影響
	異動		
2. 完整性	初估	高	本系統目的在提供車輛未繳費資料查詢服務，若資料未妥適保存或發生資安事件造成資料外洩，可能造成資料完整性受損
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	中	本系統資料包含車號與未繳費資料明細等，應依「個人資料保護法」規定辦理
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供汽機車未繳費資料查詢等對外資訊服務，屬機關業務類系統
	異動		

「全球資訊網(參考範例)」安全等級評估表

功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。

業務屬性：□行政類■業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
普	普	普	普	普
		資訊系統安全等級：		普

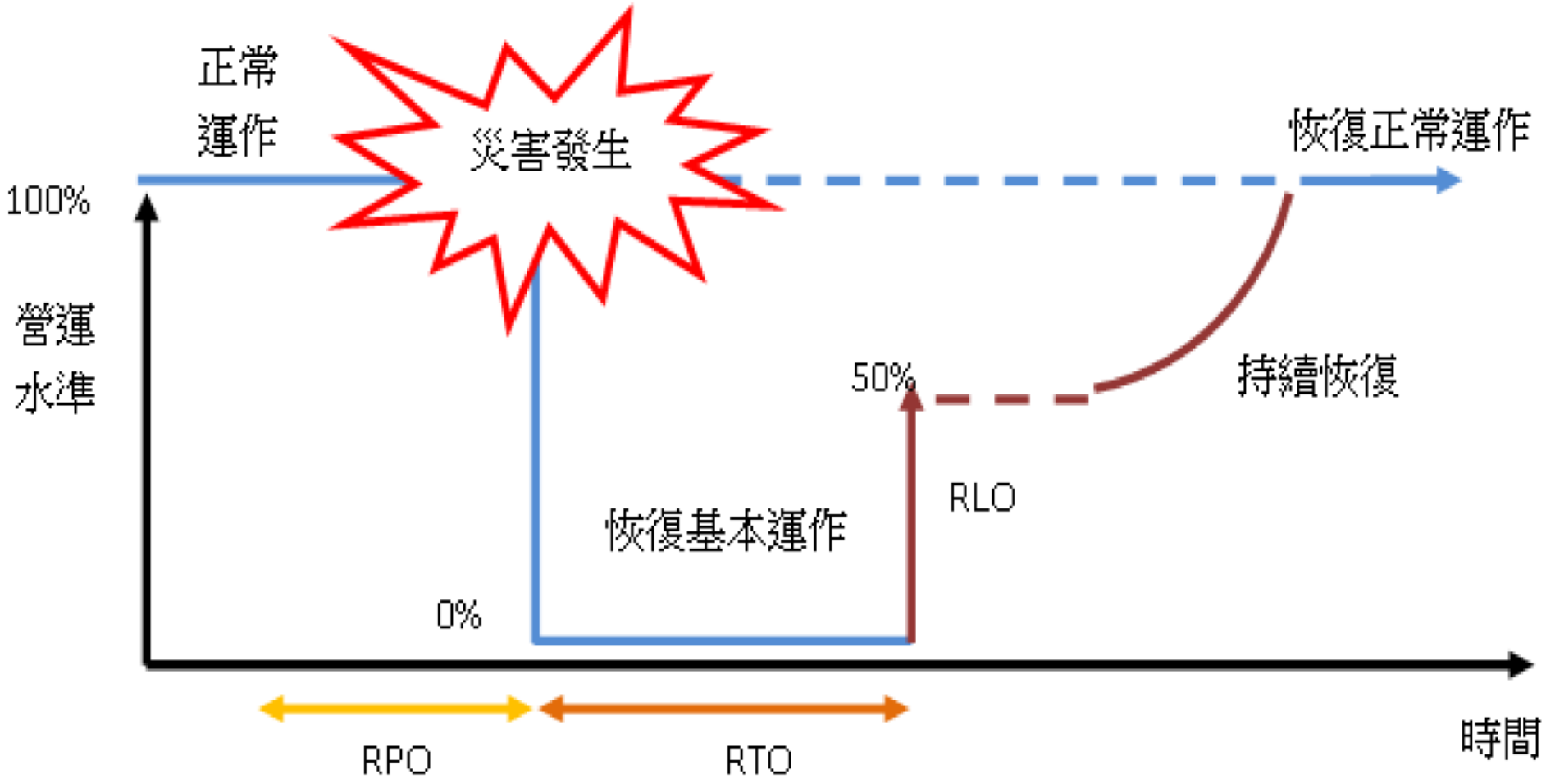
步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2. 完整性	初估	普	本網站主要提供資訊公告
	異動		
3. 可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4. 法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

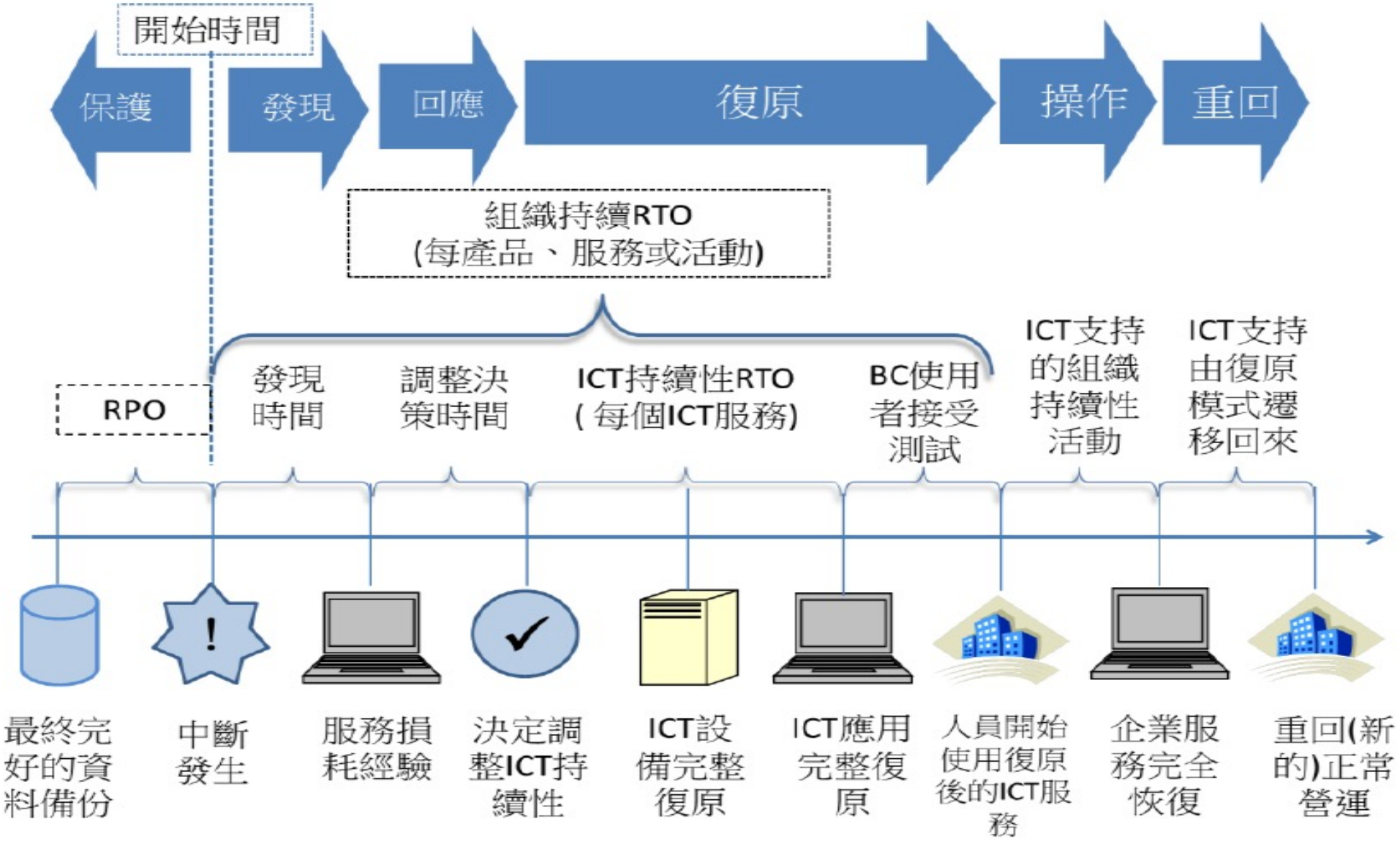
步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供機關簡介、政策措施介紹等對外資訊服務，無涉及機關業務線上申辦等其他服務，屬機關業務類系統
	異動		

最大可容忍中斷時間(一)



最大可容忍中斷時間(二)


開始時間
保護
發現
回應
復原
操作
重回
組織持續RTO
(每產品、服務或活動)
RPO
發現時間
調整決策時間
ICT持續性RTO
(每個ICT服務)
BC使用者接受測試
ICT支持的組織持續性活動
ICT支持由復原模式遷移回來
最終完好的資料備份
中斷發生
服務損耗經驗
決定調整ICT持續性
ICT設備完整復原
ICT應用完整復原
人員開始使用復原後的ICT服務
企業服務完全恢復
重回(新的)正常營運

業務流程中的資產

業務流程輸出/入

- 輸入
- 關鍵活動
- 資源
- 資源保管人
- 標準／規範
- 紀錄
- 產出
- 度量標準
- 變更

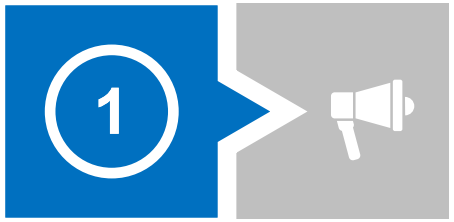
資產

- 資訊輸入
- 資訊輸出
- 資訊紀錄
- 資源
  - 人員
  - 實體設備
  - 軟體/工具
  - 通訊服務
  - 規範

規範

- 法令
- 條例
- 客戶
- 組織
  - 政策
  - 標準
  - 程序

範例(網站)



輸入：
網站資料
網站管理者

關鍵活動：新增刪除修改網站資料
資源：
網站軟體(應用、作業系統)
網站硬體(伺服器、儲存設備、網路)
維護廠商
規範(維護操作手冊)

輸出：
網頁內容
系統紀錄

鑑別

機密等級：一般			I-2-08-01資訊資產清冊						版次：V1.0			
資產編號	財產編號	資產名稱	類別	資產說明	數量	權責單位	保管單位/負責人	使用單位	機密性(C)	完整性(I)	可用性(A)	資產價值(C+I+A)

資產清點步驟

鑑別

以業務流程為主軸，由資產保管人審視與其業務相關之資產，以鑑別資產以及其他與資訊安全管理有關的資產與相對應之資產價值。

每年至少進行一次資訊資產清單覆核，以更新及確保資訊資產清單之正確性及完整性

分類　分級

依資訊資產之價值、對組織運作的關鍵程度或依其可用性和完整性進行分類。訊資產依其性質不同分類，區分為6種：包含人員、軟體、硬體、資訊紀錄、通信服務、環境等

評鑑價值

依流程及資產保管人對流程或資產影響的認知程度制訂，或是使用者發生損失、竊盜、無法使用、貪污或其他的安全侵害之考量。資產價值有三個主要的考慮部份，分別為：機密性（C）、完整性（I）、可用性（A）

確認

資產價值等級 = 機密性(C)、完整性(I)、可用性(A)三者相加。

編號標示

機密程度大於3的資訊及系統之輸出資料，應標示適當的機密等級以利使用者遵循。

應納入標示機密等級之項目，包括文件、表單。

業務類別

依據「傳播事業資通安全管理手冊」，本公司之事業體或部門，調查傳播事業營運所需之資產群組，區分為以下三項業務類別，於每年初依據管理手冊完成資通安全等級評估，並依自我評估結果，製作相關表單

代號	業務類別
A	關鍵業務類
B	支援業務類
C	行政業務類

關鍵業務類資產：無線電視事業之發射設備、傳輸鏈路、主控臺等。

支援業務類資產：指廣播電視節目供應業務及支援傳播事業應運所需之資訊處理設施，但非屬關鍵業務者，例如：客服管理系統、帳務管理系統，或事涉及客戶個人資料蒐集、處理及利用者。

行政業務類資產：指傳播事業內部輔助單位之業務項目，例如：人事、行政、總務等之業務資產。

分類 (一)

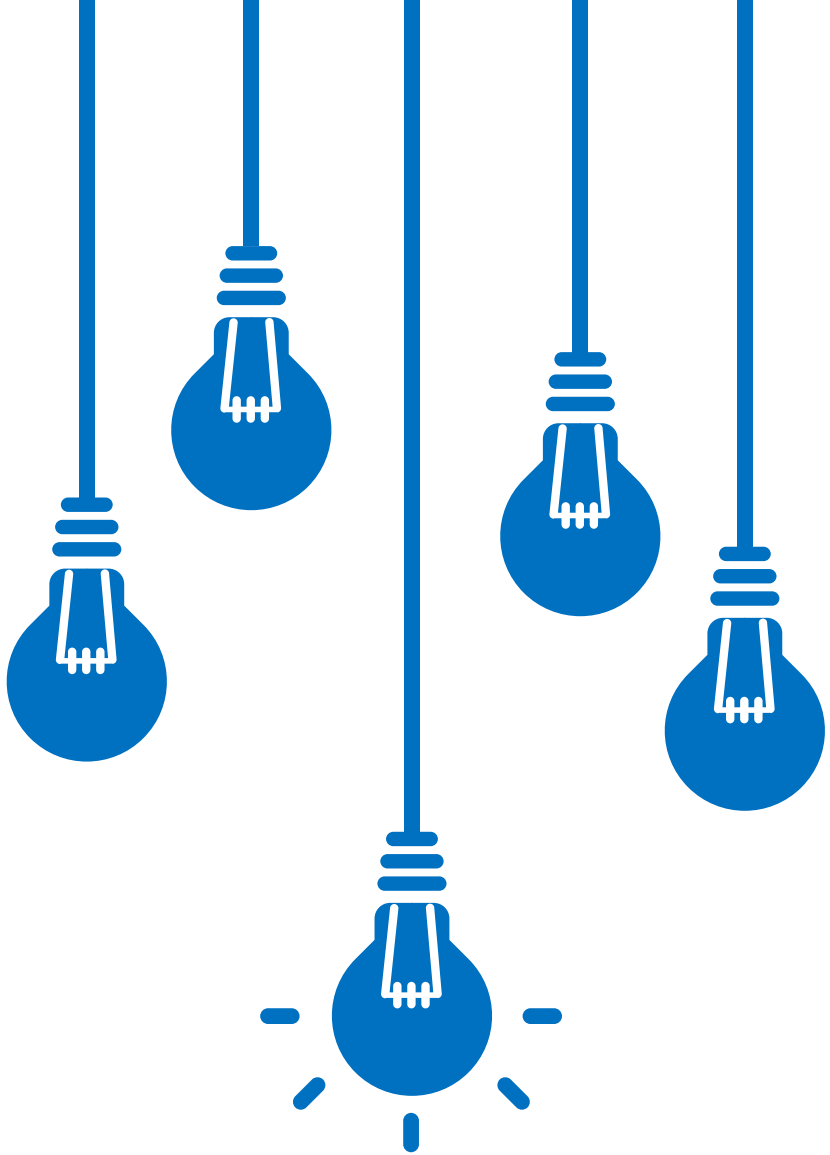
大分類	小分類	範例
人員類 （People / PE）	編制內人員	正式編制人員、臨時人員、工讀生專案人員、委外廠商.....等。
	臨時鐘點人員	
	委外廠商駐點人員	
	委外廠商	
資訊類 （Information / IF）	作業文件	資料庫與資料檔案、備份資料、原始程式碼、網路架構圖、系統文件操作或支援程序、使用手冊、教育訓練教材、管理制度文件、緊急應變&復原計畫、營運持續計劃（BCP）、稽核日誌、契約與協議報表、表單記錄.....等。
	系統文件	
	契約	
	資訊紀錄 （電子/紙本）	
	系統紀錄（Log）	

分類(二)

大分類	小分類	範例
硬體類 （Hardware / HW）	個人電腦	一般硬體：包含電腦設備（伺服器、筆記型電腦、個人電腦、工作站）、CD/DVD 燒錄器、CD/DVD光碟機、磁帶機、軟碟機、投影機、PDA、印表機……等。 通訊設備：集線器、橋接器、網路交換器、路由器、數據機、電話自動交換機（PBX）、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機。 儲存媒體：CD/DVD（空白）、硬碟（無資料）、磁片（空白）、磁帶（空白）、移動式硬碟（空白）、錄音/影帶（無資料）……等。
	可攜式電腦	
	伺服器	
	資安設備	
	網路設備	
	可攜式儲存媒體	
	電腦保護設施	
	其他硬體	

分類

大分類	小分類	範例
軟體類 （Software / SW）	作業系統	應用系統軟體、作業系統軟體、開發工具、套裝軟體、公用程式、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統（DBMS）、加密軟體、文件管理系統、內部開發程式、內部發展系統……等。
	應用系統	
	套裝軟體	
	軟體開發工具	
	資通安全系統	
環境保護類 （Environment / EV）	一般辦公區域	建築類：電腦機房、會議室、辦公室、監控室、接待區、交貨區/裝載區……等。 環境保護設施：不斷電系統、第二電力供應迴路、穩壓器、機櫃、避雷裝置、警報系統、備用發電系統、環境控制系統（火偵測、熱偵測、水偵測、溫濕度偵測、自動消防滅火系統）……等。
	特殊辦公區域	
	資訊機房	
	倉庫/庫房	
	建築保護設施	



資產價值（C、I、A）

資訊資產管理單位應鑑別其所管轄內所有資訊資產之價值。資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性。

分類

依資訊資產之特性，分成人員與非人員（含硬體、軟體、資訊及環境保護類）兩大類，其各所對應之機密性、完整性及可用性之定義與價值評估標準

機密性（Confidentiality，簡稱C）

確保只有經過授權的人才能存取資訊（使資訊不可用或不揭露給未經授權之個人、個體或過程的性質）

完整性（Integrity，簡稱I）

保護資訊及其處理方法的準確性（accuracy）和完整性（completeness）的性質。

可用性（Availability，簡稱A）

確保經授權的使用者，在需要時可以隨時存取資訊並使用相關資訊資產。

人員類資資產價值等級表

價值	機密性（C）	完整性（I）	可用性（A）
3	其工作執掌可存取限定資料（含機敏、內部使用及一般等三類）。	■ 未正確執行業務而造成資料不完整，會對業務造成很大的衝擊，甚至造成業務中斷失敗。 ■ 可能影響全組織對外所提供的服務作業。	■ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為4小時。 ■ 業務高度仰賴該員，且一旦該員無法作業時，將影響本公司對外所提供的服務作業。
2	其工作執掌可存取內部使用類資料及一般類資料。	■ 未正確執行業務而造成資料不完整，可能對業務運作不造成中斷，但降低運作效率及影響。 ■ 可能影響單一部門運作。	■ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為12小時以內。 ■ 業務仰賴該員，且一旦該員無法作業時，將影響本公司多數部門作業。
1	其工作執掌僅可存取一般類資料。	■ 未正確執行業務而造成資料不完整，可能對業務運作不會造成中斷或雖降低效率但不會造成影響。 ■ 僅僅影響少數承辦人的作業。	■ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為24小時以上。 ■ 業務仰賴該員，且一旦該員無法作業時只影響少數承辦人員作業，其工作可暫時委由他人替代。

非人員類資產價值等級表

價值	機密性（C）	完整性（I）	可用性（A）
3	▪ 機密或敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。 ▪ 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運資產或信譽等方面將產生非常嚴重或災難性之影響。	▪ 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。 ▪ 發生資通安全事件可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	▪ 僅容許短暫時間（4小時內）無法使用，作業停頓期間極易產生客訴事件，使本公司受到損害者。 ▪ 作業完全仰賴資訊資產，且一旦服務中斷時將影響全組織對外所提供的服務作業。 ▪ 發生資通安全事件可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。
2	▪ 非公開使用之非敏感性資訊處理設施與系統資源僅開放給內部人員使用。 ▪ 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運資產或信譽等方面將產生嚴重之影響。	▪ 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。 ▪ 發生資通安全事件可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	▪ 容許較長時間（8小時內）無法使用，會造成部份人員之抱怨，使本公司受到輕微損害者。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響部門運作。 ▪ 發生資通安全事件可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。
1	▪ 不限制使用資訊處理設施與系統資源等。 ▪ 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運資產或信譽等方面將產生有限之影響。	▪ 不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。 ▪ 發生資通安全事件可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。	▪ 容許長時間（1天以上）無法使用，作業停頓期間可利用其他替代方案，不致造成本公司之損失。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響少數承辦人作業。 ▪ 發生資通安全事件可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。

資產機密性等級

分級	評估標準說明
機敏	▪ 含機密或敏感資訊，僅提供少數相關業務承辦人員及其主管，或被授權之單位及人員使用。 ▪ 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。 ▪ 資訊資產存取權限須經由高階主管核准同意。
內部使用	▪ 含部分敏感資訊，僅供組織內部人員或被授權之外部單位使用。 ▪ 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。 ▪ 資訊資產存取權限須經由單位權責主管核准同意。
一般	▪ 為一般性資料可對外公開，但須遵守相關發布流程。 ▪ 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。 ▪ 資訊資產存取權限只須經由資訊資產使用者同意。

資訊資產清單及價值確認

每年至少進行一次資訊資產清單覆核，以更新及確保資訊資產清單之正確性及完整性

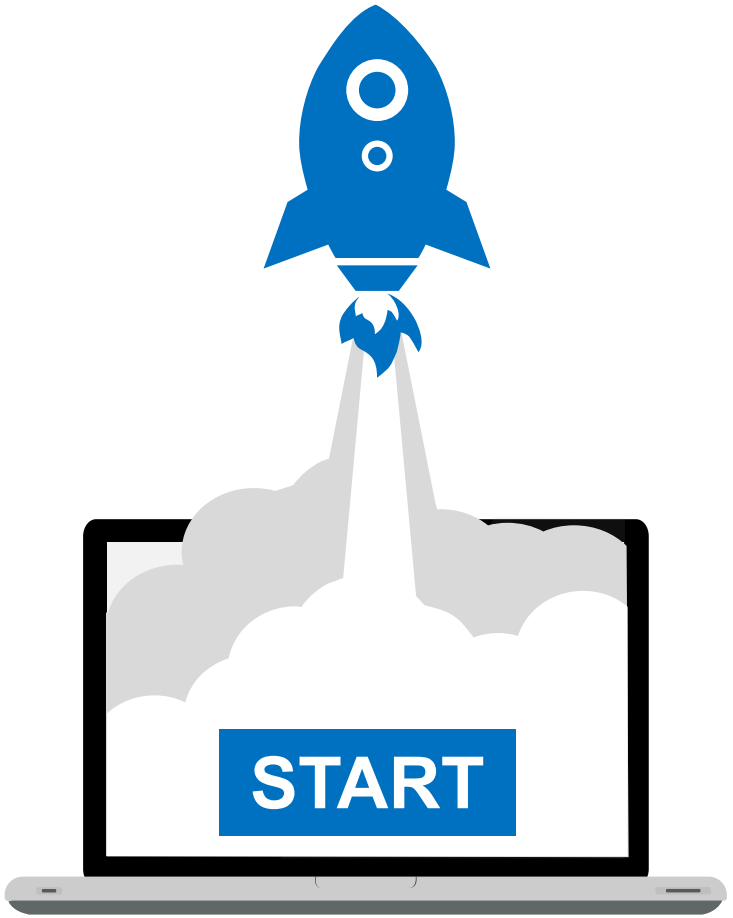
當範圍內有以下狀況發生時，則實施不定期之覆核，以更新及確保資訊資產清單之正確性及完整性。

(1)有新增、變更或移除資訊資產。

(2)系統有重大異動。

(3)作業環境改變。

資產編號及標示



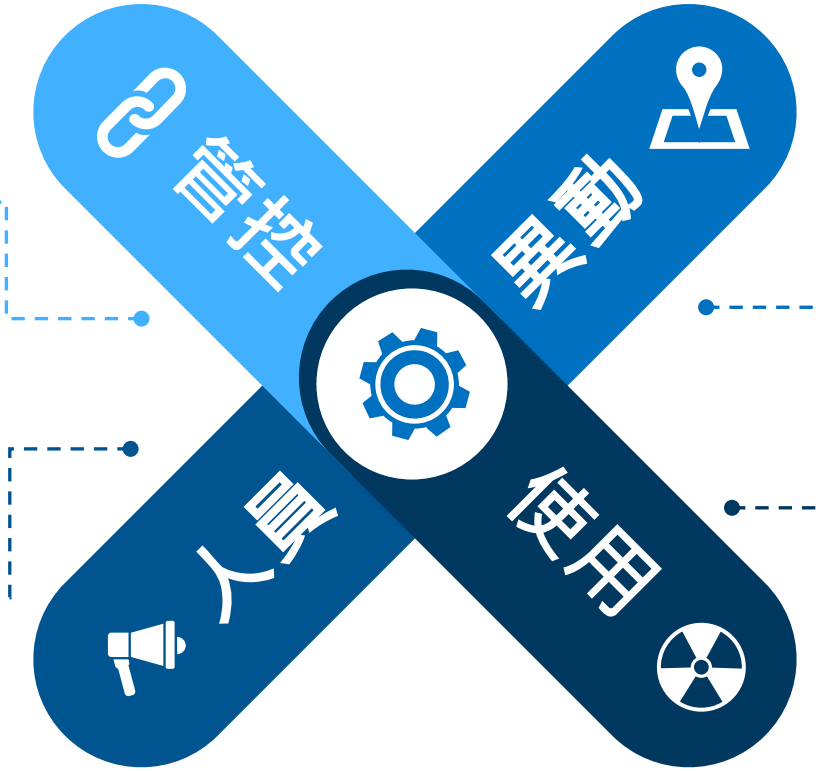
機密程度大於3的資訊及系統之輸出資料，應標示適當的機密等級以利使用者遵循。

- 表單
- 文件

資訊資產管理

文件、紀錄、相關電子檔及儲存媒體
人員之控管
實體資產（包括：軟體、硬體、環境保護等）控管

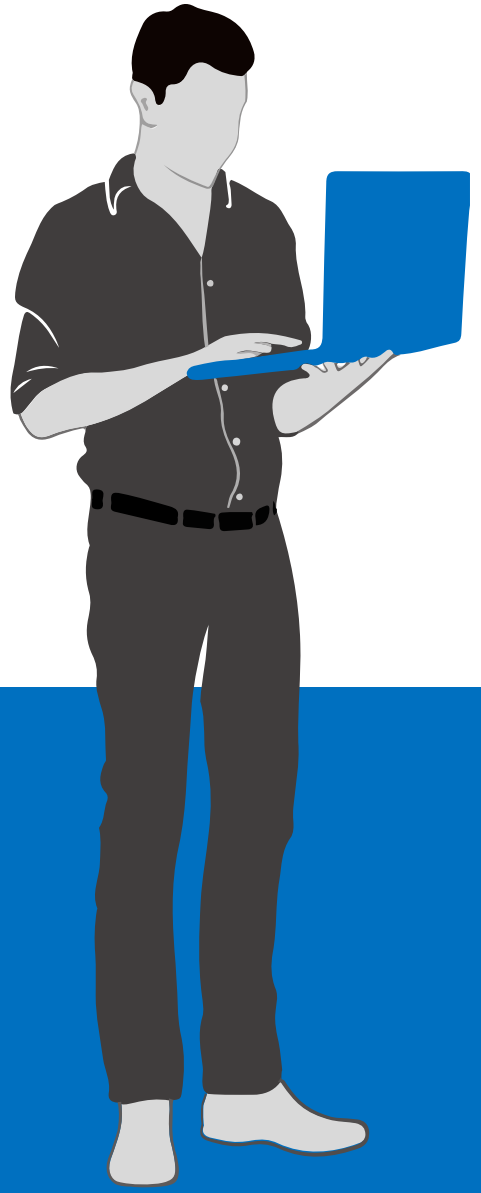
網路設備與設定、應用程式與軟體異動時應遵循「系統開發與維護管理程序書」、「系統與網路安全管理程序書」規定辦理

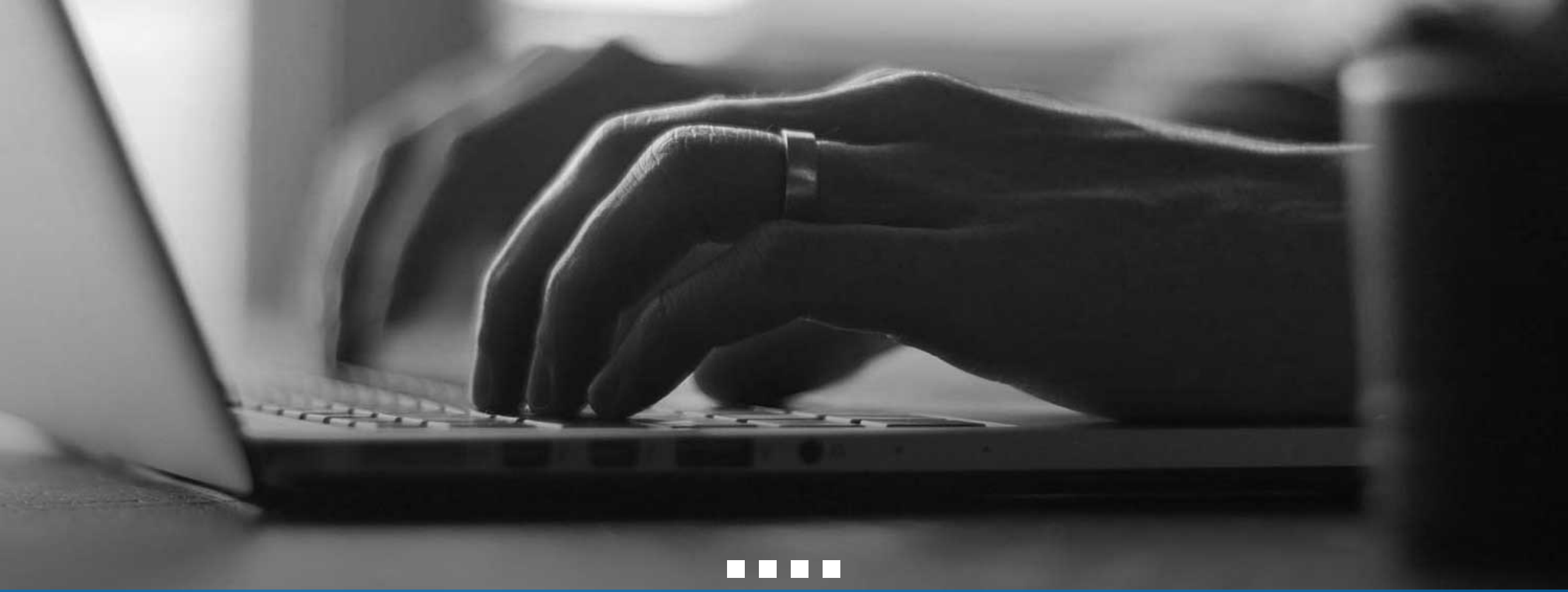


人員有異動時應遵循本府「人力資訊安全管理程序書」辦理

硬體設備如需進入機房應遵循「實體安全管理程序書」規定辦理。
文件處理應遵循「文件與紀錄管理程序書」規定辦理。
服務異動時依合約規定服務等級之要求履約並應遵循「委外程序書」規定辦理。

What is next





THANK YOU

Insert the Sub Title of Your Presentation