資訊系統分類分級鑑別機制介紹與實作

資料準備：NII產業發展協進會
講師：吳昭儀　資深經理
參考資料：「資訊系統分類分級與鑑別機制」行政院國家資通安全會報林宜燕

背景

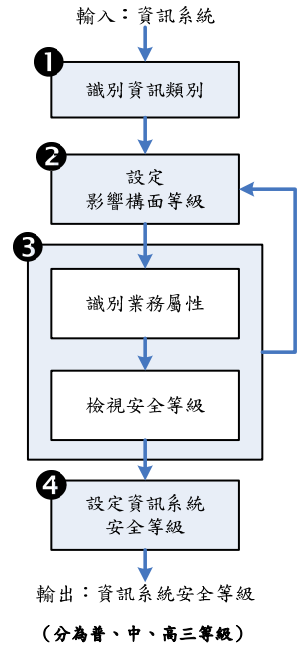
- 依據：98年1月9日行政院核定「國家資通訊安全發展方案（98年至101年）」行動方案7－推動資訊與資訊系統分類分級
  - 執行要點：
    - 整合機關、資訊及資訊系統之分類分級作法
    - 建立分類分級標準，設定基本資安防護需求水準
    - 對資訊與資訊系統進行分類分級鑑別，並要求達到最基本的資安防護需求
- 目的：旨在提供資訊系統安全等級鑑別，以協助機關掌握重點保護標的，並促使機關有效利用資源，採行適當安全控制措施，以確保各項資訊作業之安全水準

適用範圍

- 本機制適用於各級政府機關、公營事業機構、公立研究機構、學校等（以下簡稱機關）之資訊系統，涉及國家機密者應依國家機密保護法相關規定辦理
- 資訊系統定義：
  - 為協助組織決策、協調、控制、分析與實行，負責蒐集、處理、傳送、儲存與流通資訊的一組資產
    - 資產為對組織有價值的任何事物，包含資訊、軟體資產、實體資產、服務、人員、無形資產等形式

鑑別機制處理程序

- 各資訊系統均須依循處理程序填寫「安全等級評估表」
- 步驟❶：資訊類別即為施政分類（定義詳見行政院秘書處彙編「行政院施政分類架構」），資訊系統依其處理資料之性質，可包含多項資訊類別
- 步驟❷：依資料保護、業務運作、法律規章、人員傷亡、組織信譽、其他（如：財物損失）等六大構面，分別評估對各資訊類別之影響衝擊，並設定影響構面等級
- 步驟❸：依據資訊系統之業務屬性（分為關鍵性業務、支援性業務、行政性業務三類），檢視安全等級之合理性
- 步驟❹：資訊系統安全等級經資訊主管、業務主管確認後，由資訊安全長核定



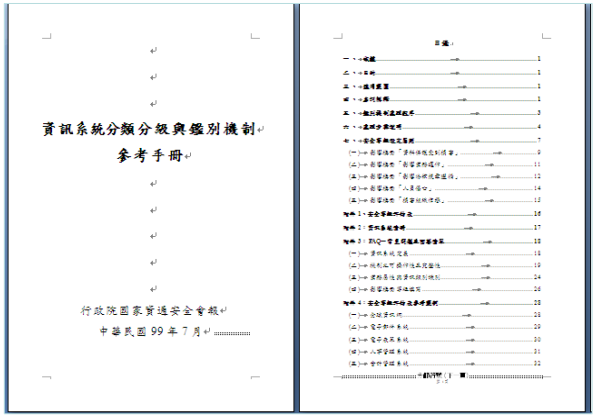
參與者

處理步驟	參與者
步驟❶：識別資訊類別	**業務承辦人**
步驟❷：設定影響構面等級	**業務承辦人**
步驟❸： -1 識別業務屬性 -2 檢視安全等級	承辦單位主管（或其授權人員）
步驟❹：設定資訊系統安全等級	資訊安全長、單位主管、資訊主管

註：業務承辦人係指負責該項業務之單位承辦人員，非專指資訊人員

「資訊系統分類分級與鑑別機制」實作範例

研讀參考手冊 → 整理資訊系統 → 系統安全等級評估 → 彙整資訊系統清冊 → 各相關單位複核


資訊系統分類分級與鑑別機制
參考手冊
行政院國家資通安全會報
中華民國 99 年 7 月

「資訊系統分類分級與鑑別機制」實作範例

研讀參考手冊 → 整理資訊系統 → 系統安全等級評估 → 彙整資訊系統清冊 → 各相關單位複核

- 蒐集資訊系統
- 將類似功能群組化


大學校務行政系統清單

相關系統予以群組化

本階段執行重點：
蒐集單位之資訊系統並加以群組化。

「資訊系統分類分級與鑑別機制」實作範例

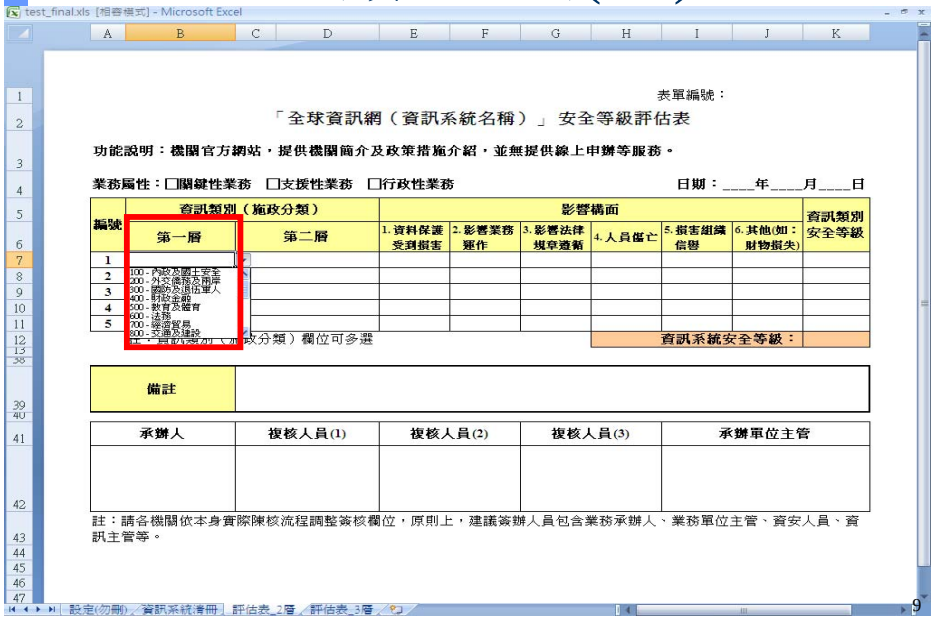
研讀參考手冊 → 整理資訊系統 → 系統安全等級評估 → 彙整資訊系統清冊 → 各相關單位複核

- 識別資訊類別
- 設定影響構面等級
- 識別業務屬性


「學籍系統」安全等級評估表

本階段執行重點：
鑑別各系統資訊類別、影響構面等級、業務屬性。

識別資訊類別(1/2)



表單編號：

「全球資訊網（資訊系統名稱）」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：□關鍵性業務 □支援性業務 □行政性業務　　日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他(如：財物損失)	
1									
2	100 - 內政及國土安全								
3	200 - 外交僑務及國際								
4	300 - 國防及退伍軍人								
5	400 - 財政金融								
	500 - 教育及體育								
	600 - 法務								
	700 - 經濟貿易								
	800 - 交通及建設							資訊系統安全等級：	

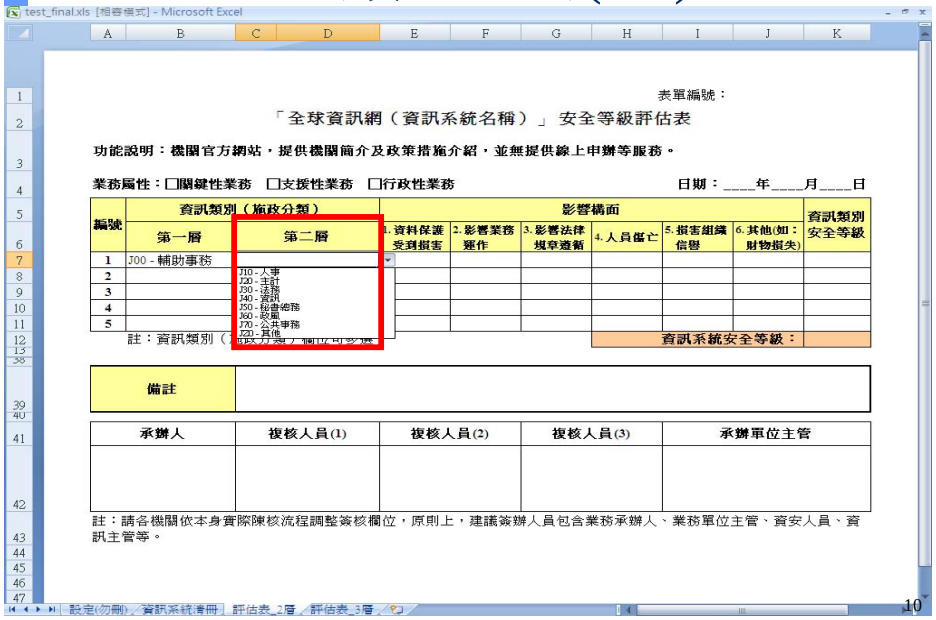
註：資訊類別（施政分類）欄位可多選

備註	

承辦人	複核人員(1)	複核人員(2)	複核人員(3)	承辦單位主管

註：請各機關依本身實際陳核流程調整簽核欄位，原則上，建議簽辦人員包含業務承辦人、業務單位主管、資安人員、資訊主管等。

識別資訊類別(2/2)



表單編號：

「全球資訊網（資訊系統名稱）」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：□關鍵性業務 □支援性業務 □行政性業務　　日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他(如：財物損失)	
1	J00 - 輔助事務								
2		J10 - 人事							
3		J20 - 主計							
4		J30 - 法務							
5		J40 - 資訊							
		J50 - 秘書總務							
		J60 - 政風							
		J70 - 公共事務							
		J99 - 其他						資訊系統安全等級：	

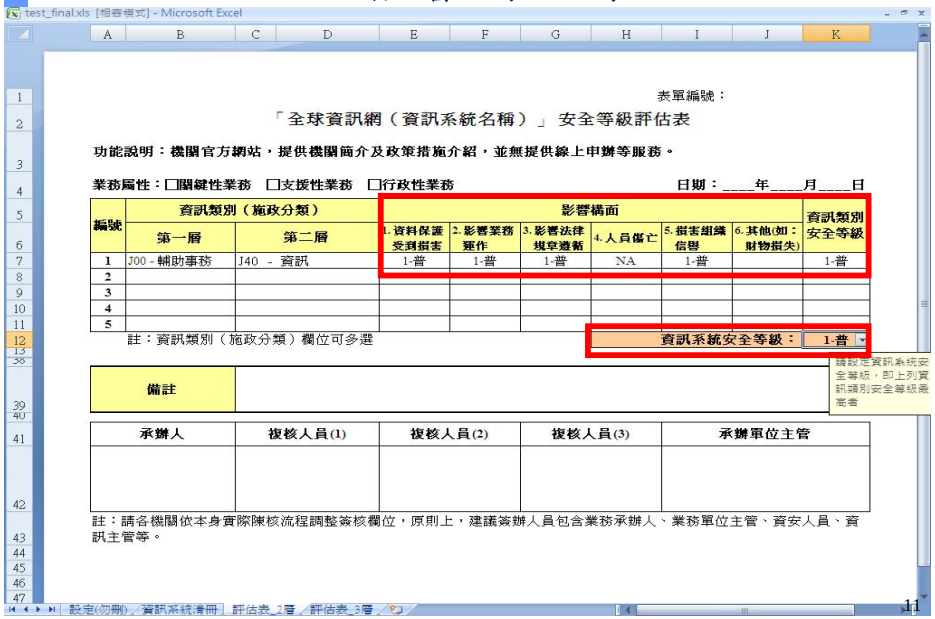
註：資訊類別（施政分類）欄位可多選

備註	

承辦人	複核人員(1)	複核人員(2)	複核人員(3)	承辦單位主管

註：請各機關依本身實際陳核流程調整簽核欄位，原則上，建議簽辦人員包含業務承辦人、業務單位主管、資安人員、資訊主管等。

設定影響構面等級



表單編號：

「全球資訊網（資訊系統名稱）」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：□關鍵性業務 □支援性業務 □行政性業務　　日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他(如：財物損失)	
1	J00 - 輔助事務	J40 - 資訊	1-普	1-普	1-普	NA	1-普		1-普
2									
3									
4									
5									
								資訊系統安全等級：	1-普

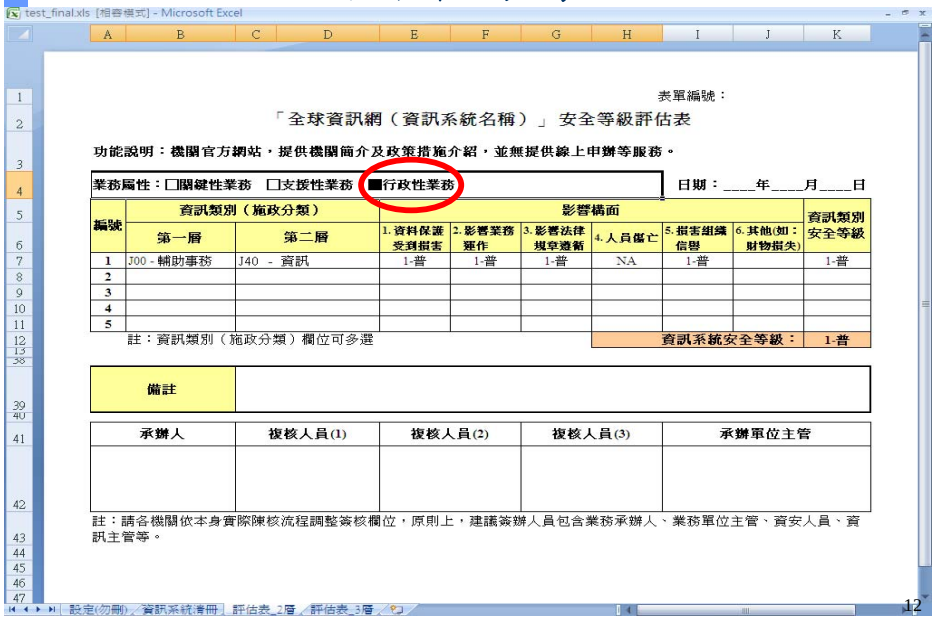
註：資訊類別（施政分類）欄位可多選

備註	

承辦人	複核人員(1)	複核人員(2)	複核人員(3)	承辦單位主管

註：請各機關依本身實際陳核流程調整簽核欄位，原則上，建議簽辦人員包含業務承辦人、業務單位主管、資安人員、資訊主管等。

識別業務屬性



表單編號：

「全球資訊網（資訊系統名稱）」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：□關鍵性業務 □支援性業務 ■行政性業務　　日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他(如：財物損失)	
1	J00 - 輔助事務	J40 - 資訊	1-普	1-普	1-普	NA	1-普		1-普
2									
3									
4									
5									
								資訊系統安全等級：	1-普

註：資訊類別（施政分類）欄位可多選

備註	

承辦人	複核人員(1)	複核人員(2)	複核人員(3)	承辦單位主管

註：請各機關依本身實際陳核流程調整簽核欄位，原則上，建議簽辦人員包含業務承辦人、業務單位主管、資安人員、資訊主管等。

安全等級設定原則(1/4)

等級 / 構面	普級（等級1）	中級（等級2）	高級（等級3）
1.資料保護受到損害	• 一般性資料 • 資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損	• 敏感性資料 • 資料若外洩或遭竄改，將導致個人權益嚴重受損	• 機密性資料 • 資料若外洩或遭竄改，將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損
2.影響業務運作	• 系統容許中斷時間較長 • 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響 • 系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低	• 系統容許中斷時間短 • 系統故障對社會秩序、民生體系運作將造成嚴重影響 • 系統故障將造成機關核心業務執行效能嚴重降低	• 系統容許中斷時間非常短 • 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全 • 系統故障將造成機關核心業務執行效能非常嚴重降低，甚至業務停頓

安全等級設定原則(2/4)

等級 / 構面	普級（等級1）	中級（等級2）	高級（等級3）
3.影響法律規章遵循	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關從根本上違反法律規章
4.人員傷亡	-	若系統發生資訊安全事故，無法完全排除造成人員傷亡的可能性	若系統發生資訊安全事故，可能造成人員死亡，或非常可能造成人員肢體傷害的危險

安全等級設定原則(3/4)

等級 / 構面	普級（等級1）	中級（等級2）	高級（等級3）
5.損害組織信譽	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害（如：導致全國性媒體報導負面新聞、造成民眾至機關抗議或陳情等情形）	若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害（如：導致國際性媒體報導負面新聞、造成民眾大規模遊行抗爭等情形）
6. 其他	由機關視本身業務特性考量可能遭遇衝擊之影響構面（如：財物損失），並依需求和本質自行設定測量基準，若依機關業務特性評估，機關可能遭遇之衝擊均已包含於前五個影響構面，則本影響構面得免填		

安全等級設定原則(4/4)

- 機關必須視本身之業務特質，自行調整設定相關數值，以符合機關之需求和本質
  - 例如：於影響構面「2.影響業務運作」，定義「系統容許中斷時間非常短」是指容許系統中斷時間不超過1小時之資訊系統
- 若資訊系統於遭遇各項資訊安全事故時，對前五個影響構面並不造成任何危害，則該影響構面等級以NA表示不適用

「資訊系統分類分級與鑑別機制」實作範例

研讀參考手冊 → 整理資訊系統 → 系統安全等級評估 → 彙整資訊系統清冊 → 各相關單位複核

資訊系統清冊

表單編號：

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	資訊系統安全等級	承辦單位	承辦人	備註
1	學籍管理系統	關鍵性業務	3-高			
2	成績管理系統	關鍵性業務	3-高			
3	學生綜合紀錄管理系統	關鍵性業務	3-高			
4	選課系統	關鍵性業務	2-中			
5	課務管理系統	關鍵性業務	1-普			
6	招生管理系統	行政性業務	2-中			
7	學生宿舍資料管理系統	行政性業務	2-中			
8	助學貸款減免管理系統	行政性業務	2-中			
9	總務管理系統	行政性業務	2-中			
10	會計管理系統	行政性業務	2-中			
11	人事管理系統	行政性業務	2-中			
12	兵役資料管理系統	行政性業務	1-普			
13	獎學金管理系統	行政性業務	1-普			
14	財產管理系統	行政性業務	1-普			
15	電話管理系統	行政性業務	1-普			
16	文書收發管理系統	行政性業務	1-普			

- 彙整資訊系統名稱
- 輸入系統業務屬性及安全等級
- 依業務屬性及安全等級排序

本階段執行重點：
將已評估完成之系統安全等級資料彙整成資訊系統清冊

教育部100年度提昇校園資訊安全服務計畫

「資訊系統分類分級與鑑別機制」實作範例

研讀參考手冊 → 整理資訊系統 → 系統安全等級評估 → 彙整資訊系統清冊 → 各相關單位複核

本階段執行重點：
1.確認系統清冊有無遺漏。
2.確認各系統安全等級評估表內容妥適性。

www.nii.org.tw

教育部100年度提昇校園資訊安全服務計畫

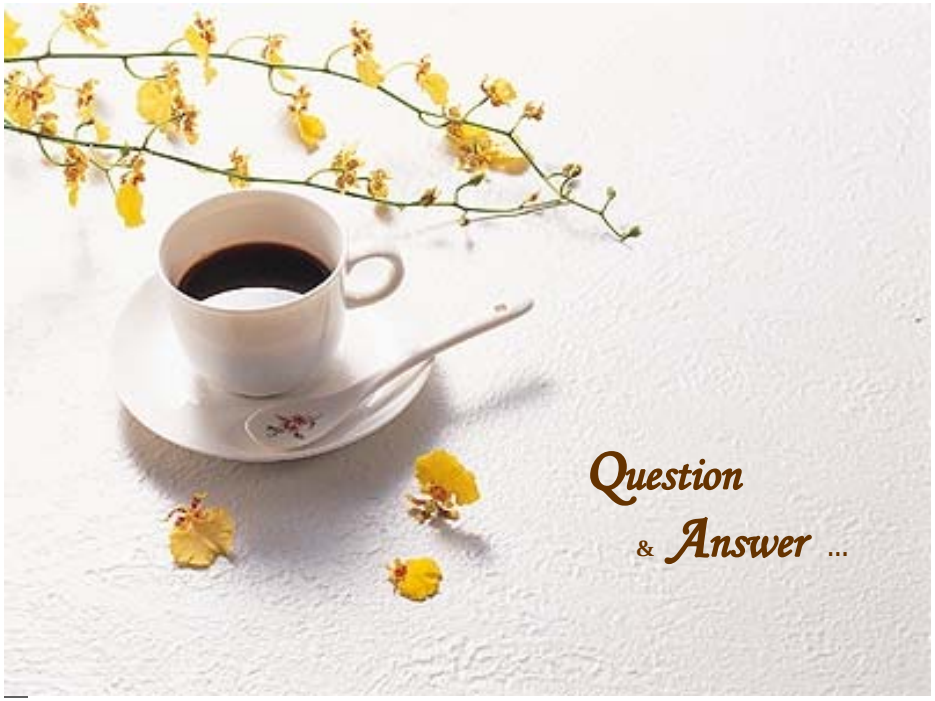
常見問題

- 安全等級分級原則較主觀，要如何建立共識？
- 通常業務單位人員參與度不足，要如何協助其進行資訊系統分類分類與鑑別？
- 若準用現行風險評估方式，是否仍要填寫「安全等級評估表」？
- 辦理完成資訊系統分類分級與鑑別，後續應如何強化系統安全？

教育部100年度提昇校園資訊安全服務計畫

結論

- 為提升機關資源利用效益，進行資訊系統分類分級與鑑別以釐清應優先保護標的，有其必要
  - A級、B級機關自100年度起，每年度應針對各資訊系統至少進行 1 次分類分級與鑑別
  - 安全等級設定原則係由機關視本身之業務特質，自行調整設定相關數值，務必符合機關之需求和本質
- 已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001等）之機關，準用現行風險評鑑方法，但須將評估結果轉為本機制之資訊系統安全等級



實作練習

請依前述介紹，試著列出單位負責的2項資訊系統，並填寫「安全等級評估表」。