下降(圖 1a)，結果也使風險等級下降(圖 1c)。

## 四、風險評鑑實作演練

第 1 節~第 3 節的觀念是重要的，第 1 節評估資訊資產 CIAL 健康度，告訴讀者每個資訊資產與生俱來就有體質健不健康的問題，主因組織認定較重要資產是不容許資安問題發生，故其健康度本質較差(指標值較高)以引起注意。第 2 節風險類型與衝擊面向，告訴讀者兩個重要名詞脆弱點與發生率的關係，「脆弱度」是由面對該風險類型衝擊之現有安全控措施程度來決定，「發生率值」則是由過去風險類型發生機率統計來決定，有時也需參考周遭環境來預測；而風險類型會衝擊資訊資產 CIAL 多個面向而非唯一。第 3 節風險評鑑方法論，告訴讀者如何選擇有效風險類型？如何利用脆弱度與發生率計算風險值？計算的風險值雖只有一個但為衝擊面向指標所共享，最後依各面向指標風險值與考慮衝擊廣度後的健康度進行風險等級計算。只有清楚上述觀念後才能實現風險評鑑撰寫技巧，底下以重要硬體資產、機敏隨身碟、機敏紙本、機敏電子檔、內部發展軟體為例，進行實際演練。

### 4.1 重要硬體資產

3kW 小型風機為國科會科專計劃，用以收集城市風力發電數據，以提供國家是否推動都會區風機設置政策。本風機架設在台南分局頂樓，高 7m 重 800kg，搜集數據供政府決策，該硬體資產本質健康度經評估為 CIAL=(0,0,2,0)，也就是僅重視其可用性問題即可，底下選擇四組風險類型，依第 3 節風險評鑑方法論進行風險評鑑報告撰寫如表 2。

(1)3.1 節選擇有效的風險類型

由於僅考慮 A 指標面向，風險類型應選擇可用性遭破壞的類型衝擊參考①(情境編號/脆弱點/威脅)，這裏可發現 2.2 節所說的相同脆弱點可面對多個不同外在威脅型態情形。

(2)3.2 節計算風險類型衝擊資產的風險值

以風險類型 1 為例，圖 2 顯示現場面對地震時，安全控制措施僅以風機

底座八顆螺絲固定明顯不足，因此脆弱度可評估最高的 3，將所觀察到的安控內容順便填入重要安控措施欄位內；發生率以過去四級地震作依據，經查本地 1 年至 3 年約發生一次，故發生率可取 2。將兩數據帶入圖 1(b)計算出風險值為 4，加上此風險類型只衝擊到 A 指標面向，可預見的風險威脅情境已明確，應將內容填寫於風險情境說明欄位內，至於 CIL 面向指標並未被衝擊到，內容上不必描述，參考②(脆弱度/發生率/風險值/重要安控措施/風險情境說明)。

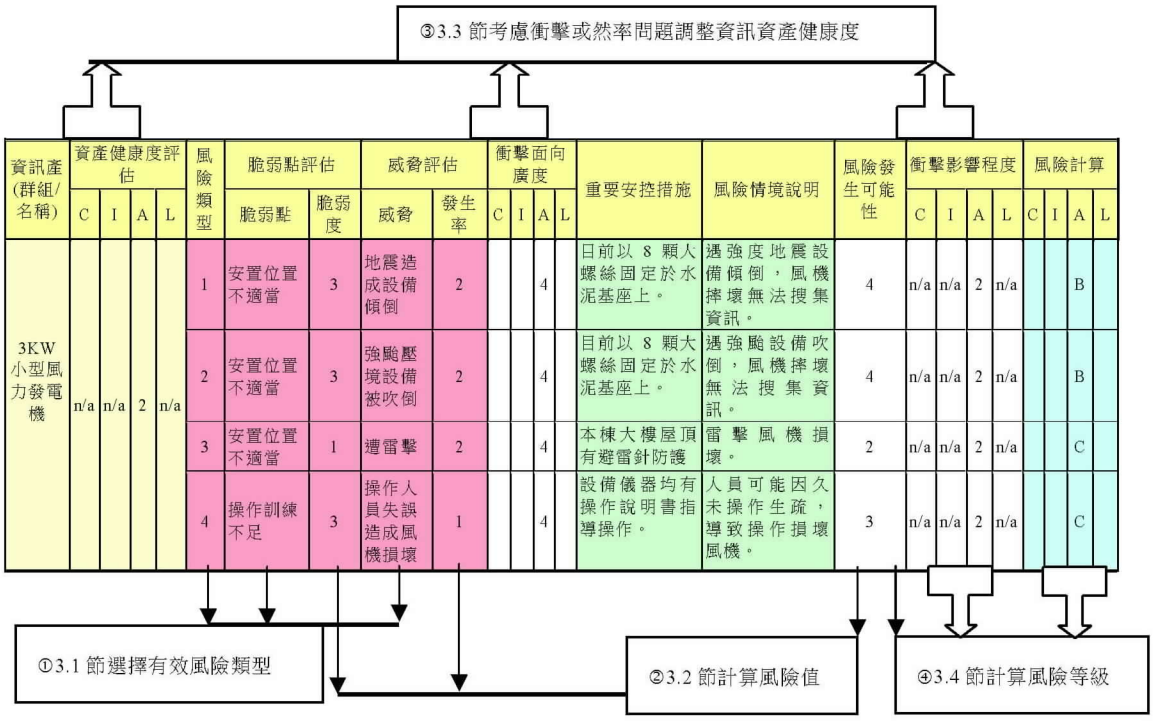
(3)3.3 節考慮衝擊廣度調整健康度

風機只有一台，損毀即不能運作，廣度可取 4(100%)，故原先健康度調整後仍為 2，參考③(資產健康度評估/衝擊面向廣度/衝擊影響程度)。

(4)3.4 節計算風險等級

因風險值僅為 A 所擁有，加入調整後的健康度，兩數據代入圖 1(c)可算出 B 級風險，參考④。

表 2 重要硬體資產的風險評鑑




| 資訊產(群組/名稱) | 資產健康度評估 | | | | 風險類型 | 脆弱點評估 | | 威脅評估 | | 衝擊面向廣度 | | | | 重要安控措施 | 風險情境說明 | 風險發生可能性 | 衝擊影響程度 | | | | 風險計算 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | L | | 脆弱點 | 脆弱度 | 威脅 | 發生率 | C | I | A | L | | | | C | I | A | L | C | I | A | L |
| 3KW小型風力發電機 | n/a | n/a | 2 | n/a | 1 | 安置位置不適當 | 3 | 地震造成設備傾倒 | 2 | | | 4 | | 日前以 8 顆人螺絲固定於水泥基座上。 | 遇強度地震設備傾倒，風機摔壞無法搜集資訊。 | 4 | n/a | n/a | 2 | n/a | | | B | |
| | | | | | 2 | 安置位置不適當 | 3 | 強颱壓境設備被吹倒 | 2 | | | 4 | | 目前以 8 顆大螺絲固定於水泥基座上。 | 遇強颱設備吹倒，風機摔壞無法搜集資訊。 | 4 | n/a | n/a | 2 | n/a | | | B | |
| | | | | | 3 | 安置位置不適當 | 1 | 遭雷擊 | 2 | | | 4 | | 本棟大樓屋頂有避雷針防護 | 雷擊風機損壞。 | 2 | n/a | n/a | 2 | n/a | | | C | |
| | | | | | 4 | 操作訓練不足 | 3 | 操作人員失誤造成風機損壞 | 1 | | | 4 | | 設備儀器均有操作說明書指導操作。 | 人員可能因久未操作生疏，導致操作損壞風機。 | 3 | n/a | n/a | 2 | n/a | | | C | |

圖 2 風險情境描述需就風險衝擊分析現場

### 4.2 儲存個資的隨身碟

儲存申訴檢舉案件調查之個資隨身碟，資訊包括身份證、地址、電話、姓名等，於本局 GIP 管理系統登打後存入電子資料庫內，除可重複呼叫印出紙本外，系統也提供轉成 word 檔之電子檔，供承辦人員存放於隨身碟備份。經附件一評估 CIAL=(3,3,2,4)各面向指標健康度不佳，屬較重要資訊資產，有較多潛在風險類型存在，底下僅選擇四組風險類型演練如表 3。

(1)3.1 節選擇有效的風險類型

CIAL 指標健康度均很差無突出者，任意風險類型選擇均有效參考①(情境編號/脆弱點/威脅)。

(2)3.2 節計算風險類型衝擊資產的風險值

以風險類型 1 為例，目前面對此風險安控措施採取「兩顆具密碼保護之隨身碟雙備份」，安控程度佳，脆弱度可評估為 1；隨身碟遺失機率有機會發生率可取 2。兩數據帶入圖 1(a)計算風險值為 2，加上此風險類型會衝擊到 CAL 指標面向(遺失洩密，洩密就觸法，遺失無法使用)，預見的風險威脅情境需就 CAL 面向均交待清楚並撰寫在風險情境說明欄位內，參考②。又風險值為 CAI 所共享故 C 風險值=A 風險值=L 風險值=2。

(3)3.3 節考慮衝擊廣度調整健康度

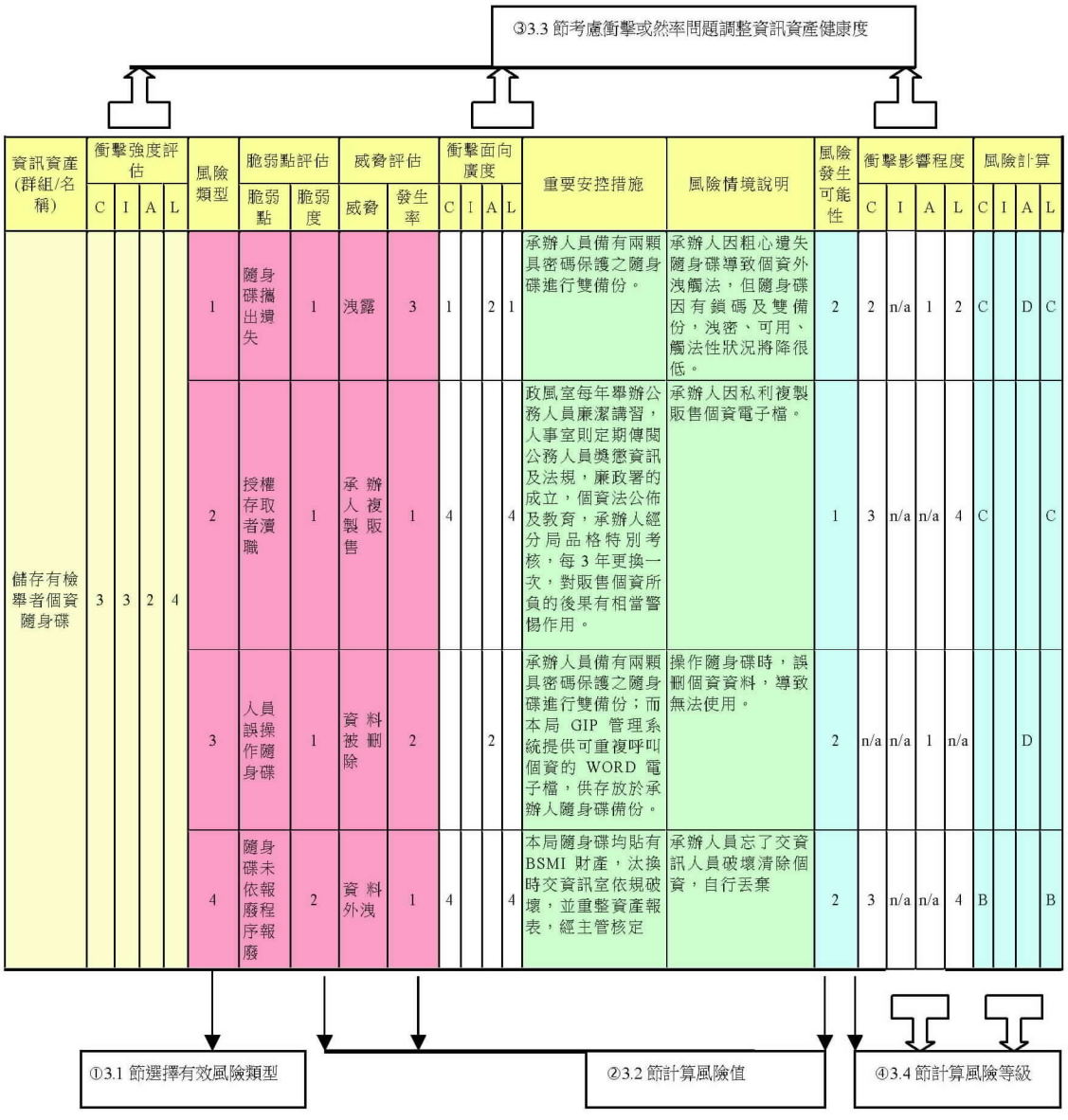
遺失洩密時因隨身碟有鎖密碼，就 C 而言其衝擊廣度不高可取 1，就 A 而言隨身碟有兩顆遺失一顆還有另一顆可用，其衝擊廣度可取 2，就 L 而言隨

身碟密碼保護洩密不易，其衝擊廣度同 C 取 1，將各面向衝擊廣度帶入圖 1(b)計算出調整後健康度為(CIAL)=(2,0,1,2)，參考③。

(4)3.4 節計算風險等級

依(2)(3)各面向風險值與調整後健康度帶入圖 1(c)，計算出風險等級為(CIAL)=(C 級，O,D 級,C 級)參考④。

表 3 具個資隨身碟的風險評鑑




| 資訊資產(群組/名稱) | 衝擊強度評估 | | | | 風險類型 | 脆弱點評估 | | 威脅評估 | | 衝擊面向廣度 | | | | 重要安控措施 | 風險情境說明 | 風險發生可能性 | 衝擊影響程度 | | | | 風險計算 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | L | | 脆弱點 | 脆弱度 | 威脅 | 發生率 | C | I | A | L | | | | C | I | A | L | C | I | A | L |
| 儲存有檢舉者個資隨身碟 | 3 | 3 | 2 | 4 | 1 | 隨身碟攜出遺失 | 1 | 洩露 | 3 | 1 | | 2 | 1 | 承辦人員備有兩顆具密碼保護之隨身碟進行雙備份。 | 承辦人因粗心遺失隨身碟導致個資外洩觸法，但隨身碟因有鎖碼及雙備份，洩密、可用、觸法性狀況將降很低。 | 2 | 2 | n/a | 1 | 2 | C | | D | C |
| | | | | | 2 | 授權存取者瀆職 | 1 | 承辦人製販售 | 1 | 4 | | | 4 | 政風室每年舉辦公務人員廉潔講習，人事室則定期傳閱公務人員獎懲資訊及法規，廉政署的成立，個資法公佈及教育，承辦人經分局品格特別考核，每 3 年更換一次，對販售個資所負的後果有相當警惕作用。 | 承辦人因私利複製販售個資電子檔。 | 1 | 3 | n/a | n/a | 4 | C | | | C |
| | | | | | 3 | 人員誤操作隨身碟 | 1 | 資料被刪除 | 2 | | | 2 | | 承辦人員備有兩顆具密碼保護之隨身碟進行雙備份；而本局 GIP 管理系統提供可重複呼叫個資的 WORD 電子檔，供存放於承辦人隨身碟備份。 | 操作隨身碟時，誤刪個資資料，導致無法使用。 | 2 | n/a | n/a | 1 | n/a | | | D | |
| | | | | | 4 | 隨身碟未依報程序報廢 | 2 | 資料外洩 | 1 | 4 | | | 4 | 本局隨身碟均貼有 BSMI 財產，汰換時交資訊室依規破壞，並重整資產報表，經主管核定 | 承辦人員忘了交資訊人員破壞清除個資，自行丟棄 | 2 | 3 | n/a | n/a | 4 | B | | | B |

### 4.3 機敏紙本

消費商品比較試驗計劃表紙本每年由總局決議後發文給分局承辦，資訊內容包括試驗單位/比較試驗名稱/品牌數/單價/試驗項目/試驗方法/試驗目的/試驗完成日，經附件一評估 CIAL=(1,2,1,1)，底下選擇四組風險類型演練如表 4。

(1)3.1 節選擇有效的風險類型

由於體質上僅 I 指標健康度略差，風險類型應選擇正確性遭惡意損毀變更的類型進行衝擊比較有效，參考①。

(2)3.2 節計算風險類型衝擊資產的風險值

以風險類型 3 為例，目前面對此風險類型的安控措施是「強化承辦人隨時上鎖來防制員工報復竄改行為」，安控程度佳，脆弱度可評估為 1；依過去 5 年此風險類型未曾發生過，發生率可取 1。兩數據帶入圖 1(a)計算風險值為 1，加上此風險類型會衝擊到 IAL 指標面向(變更正確性，損毀可用性，破壞觸法)參考②，預見的風險威脅情境需就 IAL 面向均交待清楚並撰寫在風險情境說明欄位內。又此風險值為 IAL 所共享，即 I 風險值=A 風險值=L 風險值=1。

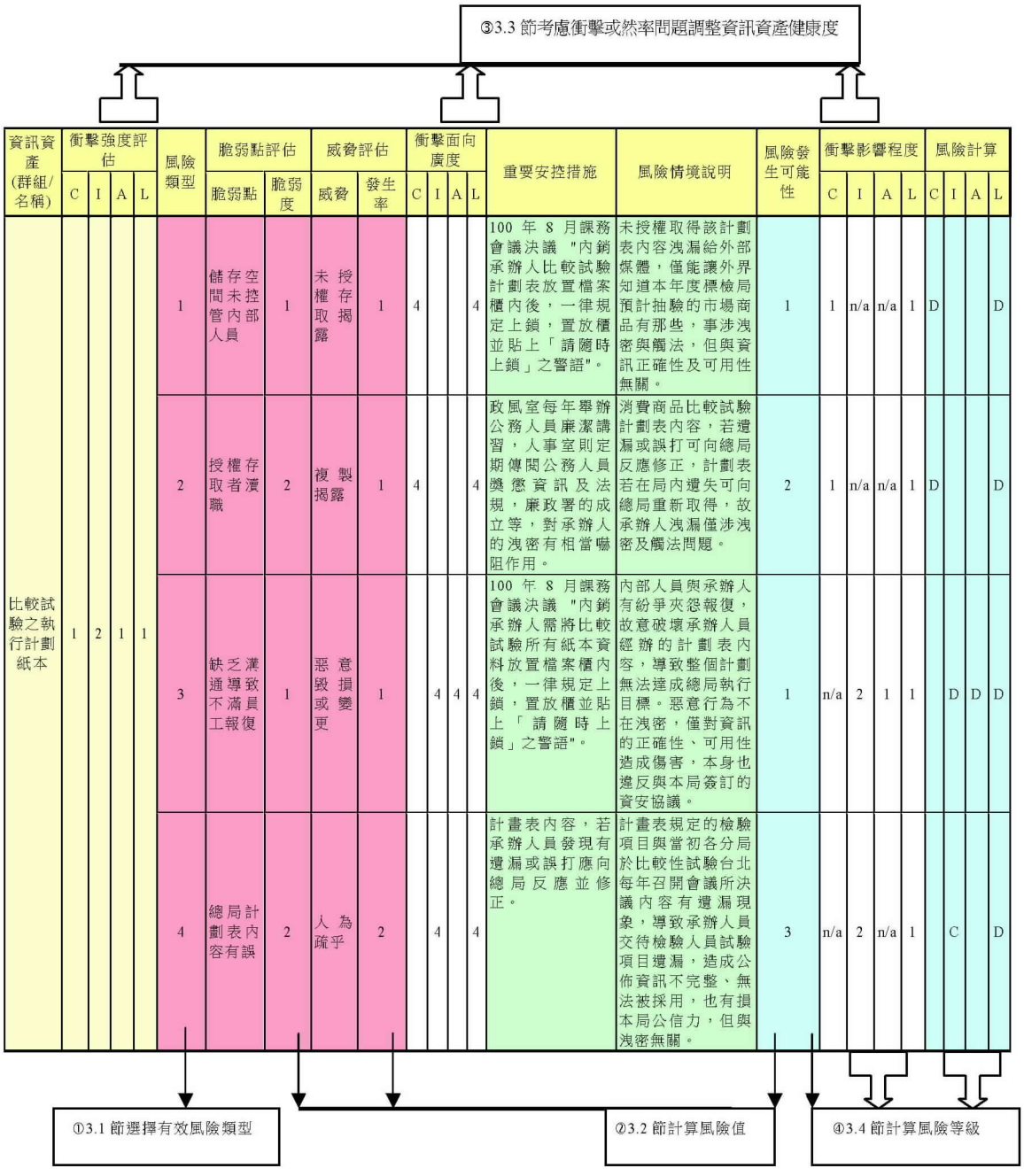
(3)3.3 節考慮衝擊廣度調整健康度

當消費商品比較試驗計劃表遭惡意損毀變更風險衝擊時，就 I 衝擊廣度而言因只有 1 份可取最高 4，就 A 衝擊廣度而言因只有 1 份也是取 4，就 L 衝擊廣度而言因破壞屬觸法並無輕重之分可取 4，將各面向衝擊廣度帶入圖 1(b)計算出調整後健康度(CIAL)=(0,2,1,1)可參考③。C=0 是因此風險類型不會衝擊到資訊的洩密性所致。

(4)3.4 節計算風險等級

依(2)(3)各面向風險值與調整後健康度帶入圖 1(c)，計算出風險等級為(CIAL)=(0 級，D 級,D 級,D 級)參考④。、

表 4 紙本的風險評鑑




| 資訊資產(群組/名稱) | 衝擊強度評估 | | | | 風險類型 | 脆弱點評估 | | 威脅評估 | | 衝擊面向廣度 | | | | 重要安控措施 | 風險情境說明 | 風險發生可能性 | 衝擊影響程度 | | | | 風險計算 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | L | | 脆弱點 | 脆弱度 | 威脅 | 發生率 | C | I | A | L | | | | C | I | A | L | C | I | A | L |
| 比較試驗之執行計劃紙本 | 1 | 2 | 1 | 1 | 1 | 儲存空間未控管內部人員 | 1 | 未授權取得揭露 | 1 | 4 | | | 4 | 100年8月課務會議決議"內銷承辦人比較試驗計劃表放置檔案櫃內後，一律規定上鎖，置放櫃並貼上「請隨時上鎖」之警語"。 | 未授權取得該計劃表內容洩漏給外部媒體，僅能讓外界知道本年度標檢局預計抽驗的市場商品有那些，事涉洩密與觸法，但與資訊正確性及可用性無關。 | 1 | 1 | n/a | n/a | 1 | D | | | D |
| | | | | | 2 | 授權存取者瀆職 | 2 | 複製揭露 | 1 | 4 | | | 4 | 政風室每年舉辦公務人員廉潔講習，人事室則定期傳閱公務人員獎懲資訊及法規，廉政署的成立等，對承辦人的洩密有相當嚇阻作用。 | 消費商品比較試驗計劃表內容，若遺漏或誤打可向總局反應修正，計劃表若在局內遺失可向總局重新取得，故承辦人洩漏僅涉洩密及觸法問題。 | 2 | 1 | n/a | n/a | 1 | D | | | D |
| | | | | | 3 | 缺乏溝通導致不滿員工報復 | 1 | 惡意毀損或更 | 1 | | 4 | 4 | 4 | 100年8月課務會議決議"內銷承辦人需將比較試驗所有紙本資料放置檔案櫃內後，一律規定上鎖，置放櫃並貼上「請隨時上鎖」之警語"。 | 內部人員與承辦人有紛爭夾怨報復，故意破壞承辦人員經辦的計劃表內容，導致整個計劃無法達成總局執行目標。惡意行為不在洩密，僅對資訊的正確性、可用性造成傷害，本身也違反與本局簽訂的資安協議。 | 1 | n/a | 2 | 1 | 1 | | D | D | D |
| | | | | | 4 | 總局計劃表內容有誤 | 2 | 人為疏乎 | 2 | | 4 | | 4 | 計畫表內容，若承辦人員發現有遺漏或誤打應向總局反應並修正。 | 計畫表規定的檢驗項目與當初各分局於比較性試驗台北每年召開會議所決議內容有遺漏現象，導致承辦人員交待檢驗人員試驗項目遺漏，造成公佈資訊不完整、無法被採用，也有損本局公信力，但與洩密無關。 | 3 | n/a | 2 | n/a | 1 | | C | | D |

## 4.4 機敏電子檔

驗證登錄報驗技術文件目前均由認可實驗室轉 PDF 檔，再上傳至本局開發之 PCM 商品驗證登錄管理系統(網路版)，系統自動下載電子檔至承辦人電腦硬碟 D 目錄並產生資料夾 EDOCdownloads。承辦人因此可打開 pdf 檔進行審查，若發現報告試驗有問題則透過系統登打補件通知單，由系統自動 E-MAIL 給實驗室與廠商補件上傳，經附件一評估 CIAL=(0,3,3,1)，底下選擇三組風險類型演練如表 5。

(1)3.1 節選擇有效的風險類型

由於體質上 IA 指標健康度差，風險類型應選擇正確性及可用性遭破壞的類型進行衝擊比較有效，參考①。

(2)3.2 節計算風險類型衝擊資產的風險值

以風險類型 4 硬碟變質損毀資料為例，目前面對此風險的安控措施是「承辦人員可自系統重複下載電子檔」，安控程度佳，強脆弱度可評估為 1；依過去 5 年此風險類型未曾發生發生率可取 1。兩數據帶入圖 1(a)計算出風險值為 1，因此風險只衝擊到 A 面向指標，風險值僅由 A 指標所有參考②。

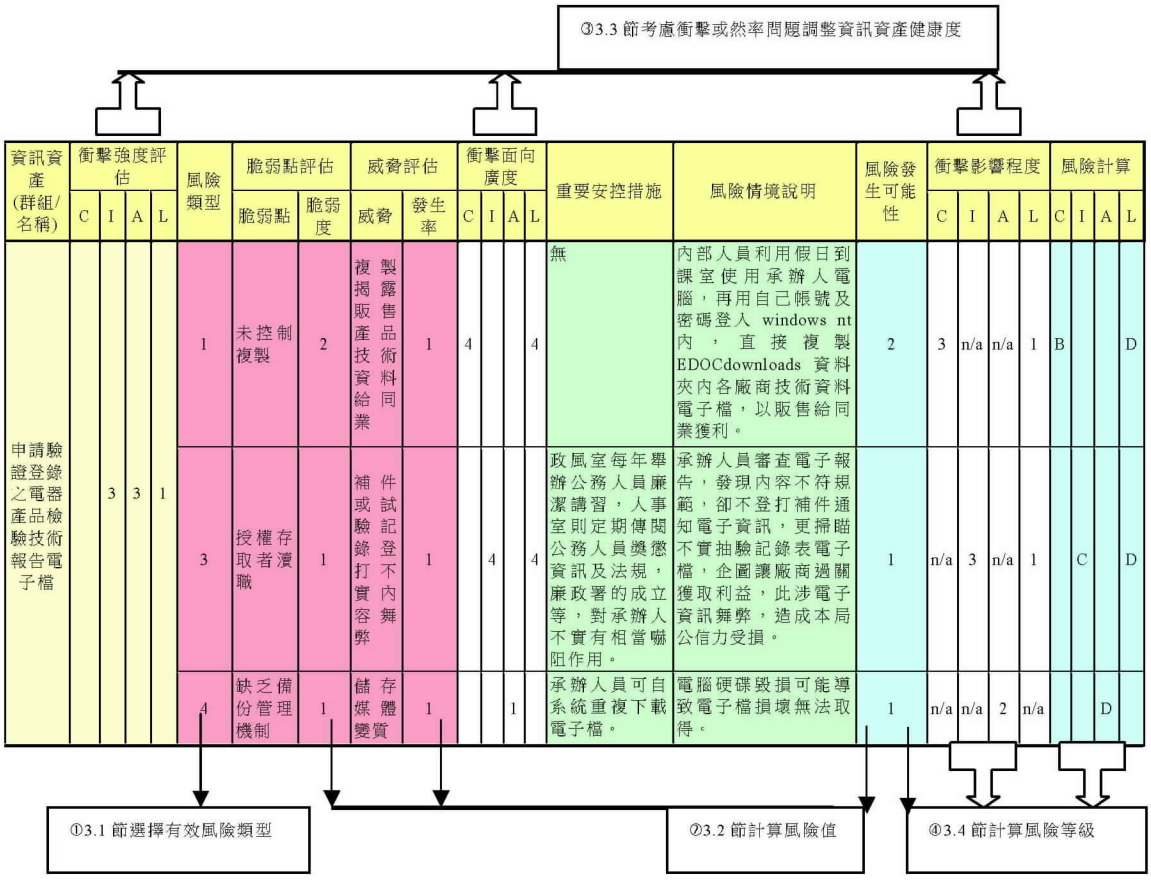
(3)3.3 節考慮衝擊廣度調整健康度

當 EDOCdownloads 資料夾因硬碟質變而損毀時，就 A 衝擊廣度而言因其可至系統重複取得，損失非全面不可得故可取 1，經帶入圖 1(b)計算調整後健康度(CIAL)=(0,0,2,0)可參考③，CIL=0 是因風險類型無衝擊到此面向指標故廣度=0。

(4)3.4 節計算風險等級

依(2)(3) 風險值與調整後健康度帶入圖 1(c)計算出風險等級為(CIAL)=(0 級，0 級,D 級,0 級)，參考④。

表 5 電子檔的風險評鑑




| 資訊資產(群組/名稱) | 衝擊強度評估 | | | | 風險類型 | 脆弱點評估 | | 威脅評估 | | 衝擊面向廣度 | | | | 重要安控措施 | 風險情境說明 | 風險發生可能性 | 衝擊影響程度 | | | | 風險計算 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | L | | 脆弱點 | 脆弱度 | 威脅 | 發生率 | C | I | A | L | | | | C | I | A | L | C | I | A | L |
| 申請驗證登錄之電器產品檢驗技術報告電子檔 | | 3 | 3 | 1 | 1 | 未控制複製 | 2 | 複製揭露販售產品技術資料給同業 | 1 | 4 | | | 4 | 無 | 內部人員利用假日到課室使用承辦人電腦，再用自己帳號及密碼登入 windows nt 內，直接複製 EDOCdownloads 資料夾內各廠商技術資料電子檔，以販售給同業獲利。 | 2 | 3 | n/a | n/a | 1 | B | | | D |
| | | | | | 3 | 授權存取者瀆職 | 1 | 補件或驗錄打實容弊 | 1 | | 4 | | 4 | 政風室每年舉辦公務人員廉潔講習，人事室則定期傳閱公務人員獎懲資訊及法規，廉政署的成立等，對承辦人不實有相當嚇阻作用。 | 承辦人員審查電子報告，發現內容不符規範，卻不登打補件通知電子資訊，更掃瞄不實抽驗記錄表電子檔，企圖讓廠商過關獲取利益，此涉電子資訊舞弊，造成本局公信力受損。 | 1 | n/a | 3 | n/a | 1 | | C | | D |
| | | | | | 4 | 缺乏備份管理機制 | 1 | 儲存體媒變質 | 1 | | | | 1 | 承辦人員可自系統重複下載電子檔。 | 電腦硬碟毀損可能導致電子檔損壞無法取得。 | 1 | n/a | n/a | 2 | n/a | | | D | |

## 4.5 內部發展軟體

風力機與太陽光電系統之資料收集軟體安裝於平板電腦，該電腦具有線上網與無線上網雙埠，而收集資料數據均累積至電腦資料庫內，該電腦有線與無線上網均已設定開啟，且軟體設計有遠端搖控功能以方便總局連線收集，經附件一評估為 CIAL=(0,0,2,1)，底下選擇三組風險類型演練如表 6。

(1)3.1 節選擇有效的風險類型

由於體質上 A 指標健康度略差，風險類型應選擇可用性遭破壞的類型進行衝擊比較有效，參考①。

(2)3.2 節計算風險類型衝擊資產的風險值

以風險類型 3 網路入侵破壞為例，目前面對此風險類型的安控措施程度

是「內部連線電腦可與該台平板電腦連線，但內部連線與外界網路由台北總局防火牆阻隔連線；至於無線上網並無安控措施」，整體仍然因無線網路出現嚴重脆弱點故脆弱度可評估為最高 3；此風險類型目前雖無發生，但從周遭環境觀察，可透過公家所提供 I-TAIWAN 無線網路輕易以筆電連線進行遠端遙控，故發生率仍可評估最高的 3。將兩數據帶入圖 1(a)計算風險值是 4。而因此風險類型僅衝擊到 A 面向指標，風險值僅為 A 指標所有參考②。

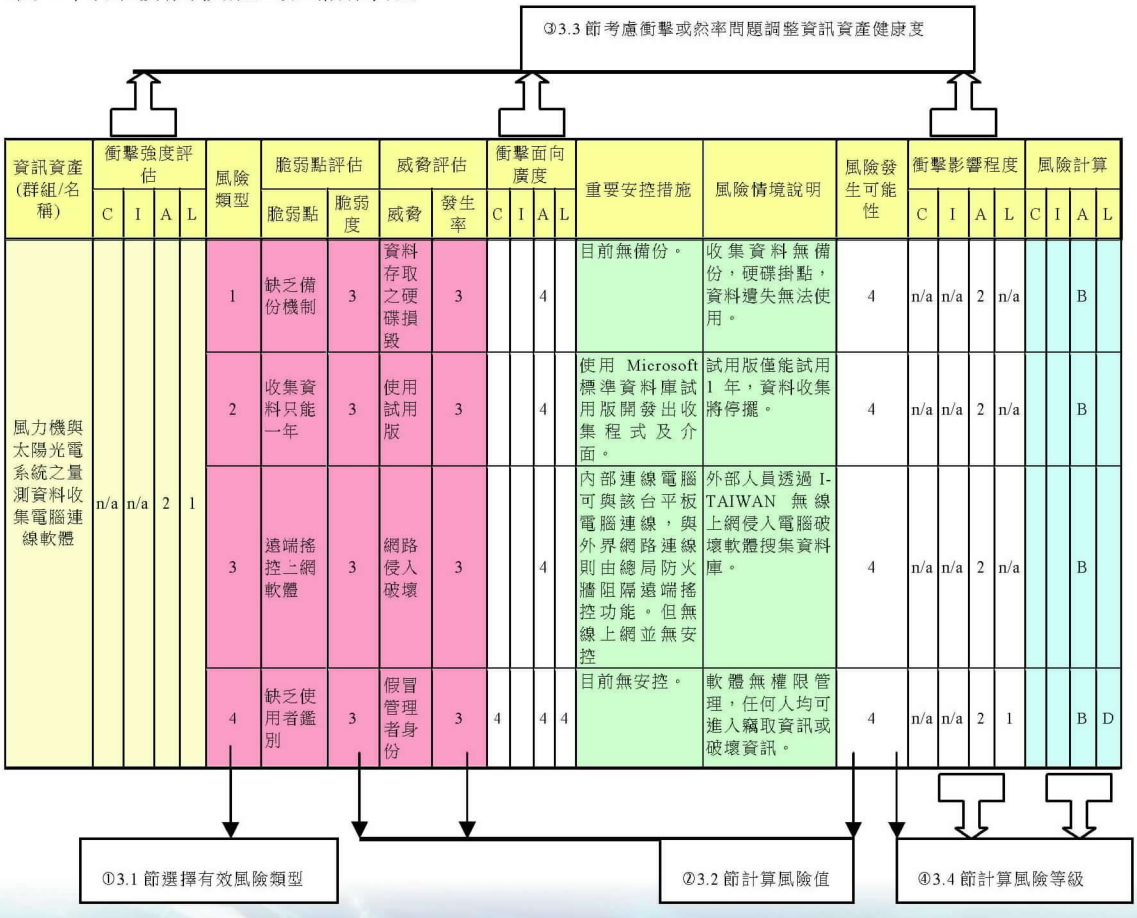
(3)3.3 節考慮衝擊廣度調整健康度

當資料庫被遠端遙控上網破壞，就 A 衝擊廣度而言是全面性的毀損，資訊無法再生故取 4，帶入圖 1(b)計算調整後健康度為(CIAL)=(0,0,2,0)參考③。

(4)3.4 節計算風險等級

依(2)(3) 風險值與調整後健康度帶入圖 1(c)計算出風險等級為(CIAL)=(0級，0 級,B 級,0 級)參考④。

表 6 內部發展軟體的風險評鑑




| 資訊資產(群組/名稱) | 衝擊強度評估 | | | | 風險類型 | 脆弱點評估 | | 威脅評估 | | 衝擊面向廣度 | | | | 重要安控措施 | 風險情境說明 | 風險發生可能性 | 衝擊影響程度 | | | | 風險計算 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | L | | 脆弱點 | 脆弱度 | 威脅 | 發生率 | C | I | A | L | | | | C | I | A | L | C | I | A | L |
| 風力機與太陽光電系統之量測資料收集電腦連線軟體 | n/a | n/a | 2 | 1 | 1 | 缺乏備份機制 | 3 | 資料存取之硬碟損毀 | 3 | | | 4 | | 目前無備份。 | 收集資料無備份，硬碟掛點，資料遭失無法使用。 | 4 | n/a | n/a | 2 | n/a | | | B | |
| | | | | | 2 | 收集資料只能一年 | 3 | 使用試用版 | 3 | | | 4 | | 使用 Microsoft 標準資料庫試用版開發出收集程式及介面。 | 試用版僅能試用 1 年，資料收集將停擺。 | 4 | n/a | n/a | 2 | n/a | | | B | |
| | | | | | 3 | 遠端搖控上網軟體 | 3 | 網路侵入破壞 | 3 | | | 4 | | 內部連線電腦可與該台平板電腦連線，與外界網路連線則由總局防火牆阻隔遠端搖控功能。但無線上網並無安控 | 外部人員透過 I-TAIWAN 無線上網侵入電腦破壞軟體搜集資料庫。 | 4 | n/a | n/a | 2 | n/a | | | B | |
| | | | | | 4 | 缺乏使用者鑑別 | 3 | 假冒管理者身份 | 3 | 4 | | 4 | 4 | 目前無安控。 | 軟體無權限管理，任何人均可進入竊取資訊或破壞資訊。 | 4 | n/a | n/a | 2 | 1 | | | B | D |

## 五、結論

人體身心健康度與否會影響人類社會的發展及運行，但人體天生體質不同，有些人面對風險威脅會發病，有些人面對同樣風險卻不會，個體生病就會影響社會運行，更多個體發病(如瘟疫)社會可能停擺。同樣的資訊世界運行由資訊資產構成，資訊資產健康受風險衝擊就是資安問題，資安有問題會使資訊世界運行受阻，更多資訊資產資安出問題產出，代表資訊世界營運會停擺。資訊世界營運與人類社會運行是一樣的，只是資訊世界較為抽象更難理解，風險評鑑作業的意義在於挖掘資訊資產面對何種風險類型衝擊，體質較弱者將發病，以便事前透過風險處理如避免、轉稼、防堵等手段來預防其失效，使資訊世界營運順暢產能加倍。本局從 95 年導入 ISMS 管理系統，97 年開始在各分局與辦事處檢驗及度量衡單位進行風險評鑑作業；續於 98 年將範圍擴充到人事、政風、會計、秘書室；99 年各課室重新風險評鑑並將適法性及個資導入；100 年再全面審視評鍵；101 年增加實驗室儀器風險評鑑及對全部資訊資產重新加入衝擊廣度計算，以貼切實際情形；102 年風險再評鑑並對新增加資訊資產執行風險評鑑作業，每年都定期重新盤點資訊資產並重新評鑑，完全符合 ISO27001 風險評鑑作業需求。

## 附件一 資訊資產的 C、I、A、L 量測

| C：資訊資產本身機密程度<br>如果被洩密，影響的對象與程度<br>(1)影響單位內部單一作業(即與其它業務流程無關)->C=1<br>(2)影響主管重要業務or洩漏個資對當事人造成不便->C=2<br>(3)影響廠商民眾權益or洩漏個資造成當事人被威脅->C=3<br>(4)影響國家權益->C=4<br>(5)沒影響到->n/a | I：資訊資產本身完整性程度，其影響層級<br>如果被竄改(偽造) or 誤打(少打、打錯) or 儀器未校正輸出不正確<br>(1)影響單位內部單一作業(即與其它業務流程無關)->I=1<br>(2)影響主管重要業務->I=2<br>(3)影響廠商民眾權益->I=3<br>(4)影響國家權益->I=4<br>(5)沒影響到 -> n/a |
|---|---|
| 機密性 C 量測 | 完整性/正確性 I 量測 |

A：當資訊資產因某種原因取得困難導致業務停擺，重新取得恢復業務時間
如果資訊系統暫停 or 遺失 or 毀損 or 硬體類遭破壞而造成業務中斷其影響
(1)影響內部作業或業務中斷->1hr≦t<4hr
(2)影響主管重要業務或業務中斷->4hr≦t<1日
(3)影響廠商民眾權益或業務中斷->1日≦t<3日
(4)影響國家權益或業務中斷->3日≦ t
(5)沒影響到->n/a

可用性 A 量測

L：當資訊資產的不當行動的適法性
有兩個層面：
(A)法律層面(即法律或組織訂定的內部規範如本局商檢法/市場監督法/Guide65/品質QMS/國家標準CNS等)
(B)形象、公信力、信譽(if組織無(A)問題可考慮B)
當C洩密 / I竄改 / A遺失，而導致違背上述規定，其追究層級可達
(1)承辦人/承辦科室->L=1
(2)單位主管or違反內部規範->L=2
(3)分局/本局or違反行政命令->L=3(如造成分局長上媒體)
(4)機關以上or違反法律->L=4(指委違反到國家法律或行政命令受罰)
(5)沒影響到->n/a

適法性 L 量測

★ 特殊：個資的C、I、A,、L判定
C：個資洩密部份，大部份取2及3：
(1)涉個資的一般業務，洩露可能造成當事人收到不想收的信件或電話，造成當事人不便-> C=2
(2)涉個資敏感性業務，洩露可能造成當事人遭恐嚇、騷擾如檢舉人、糾紛鑑定->C=3
涉員工個資的人事管理業務，洩露可能造成當事人較大的風險->C=3
委外廠商或外部人員(派駐/委外)管理的組織個資業務 ，由於不易管控，洩露衝擊很大->C=3
存於資料庫的個資，洩露出去對組織產生高衝擊->C=3
I：個資完整性，依一般資產定義判定。
A：個資可用性，依一般資產定義判定。
L：個資適法性，大部份取3及4：
(1)違反行政命令->L=3
(2)違反法律->L=4

個資的 C、I、A、L 量測