# 中央研究院

# 資訊科學研究所

## 風險評鑑作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I306

版　　本：1.0

核准日期：115 年 4 月 24 日

# 文件制／修訂紀錄表

| 版次 | 修訂日期 | 修訂單位 | 修訂者 | 核准者 | 修訂內容 |
|---|---|---|---|---|---|
| 1.0 | | | | | 新擬訂文件 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# 目錄

## 壹、目的

中央研究院資訊科學研究所（以下簡稱本所）於執行與維護資訊安全管理系統（ISMS）時，評估風險適切性、方法及步驟，以期能達到資通運用之機密性、完整性及可用性，特訂定風險評鑑作業說明書（以下簡稱本說明書）以資遵循。

## 貳、依據

一、資通安全管理法及其子法

二、中央研究院資通安全暨個人資料保護政策及規範

三、中央研究院資通安全管理規範實施要點

四、ISO/IEC 27001 資訊安全管理系統（Information Security Management System，ISMS）

## 參、範圍

本所完成盤點及價值鑑別的各項資通資產之威脅/脆弱點鑑別、風險鑑別、控制目標及控制措施鑑別，以及監視與審查。

## 肆、權責

一、 資安長

負責審查「資產清冊」、「風險評鑑」後，且核定可接受之風險值，並查核「風險處理計畫」的執行成效。

二、 資通安全推動小組

定期檢討可接受風險值與威脅及弱點評估表之項目，維護與保存「風險處理計畫」並負責執行。

三、 資通安全管理委員會

須定期或不定期查核資通安全推動小組的 ISMS 推動成效。

四、 資通資產管理單位

1. 鑑別資產的價值
2. 資產的機密性等級分類
3. 資產威脅與脆弱點的鑑別

4. 鑑別資產可忍受之最大失效期間
5. 鑑別失去資產對組織的衝擊
6. 鑑別資產的風險擁有者
7. 參與安全防護對策之討論與決策
8. 系統安全防護與系統維護之成本分析
9. 鑑別資產之特性，作為營運持續管理之參考
10. 參與營運持續計畫之討論
11. 支援營運持續演練
12. 定期與不定期重新進行風險評鑑，以鑑定安全防護計畫之成效及鑑別風險之變化與新風險的產生。

五、 資通資產使用單位

有責任向資通安全管理委員會提供與決策程序相關的資訊，包括現有或不存在的控制與對策以及可行方法或選擇。

## 伍、作業說明

本風險評鑑之方法參考國際標準進行風險評鑑。風險評鑑程序為整體 ISMS 架構的一部分，整體程序架構請參見圖 1：風險評鑑流程圖。

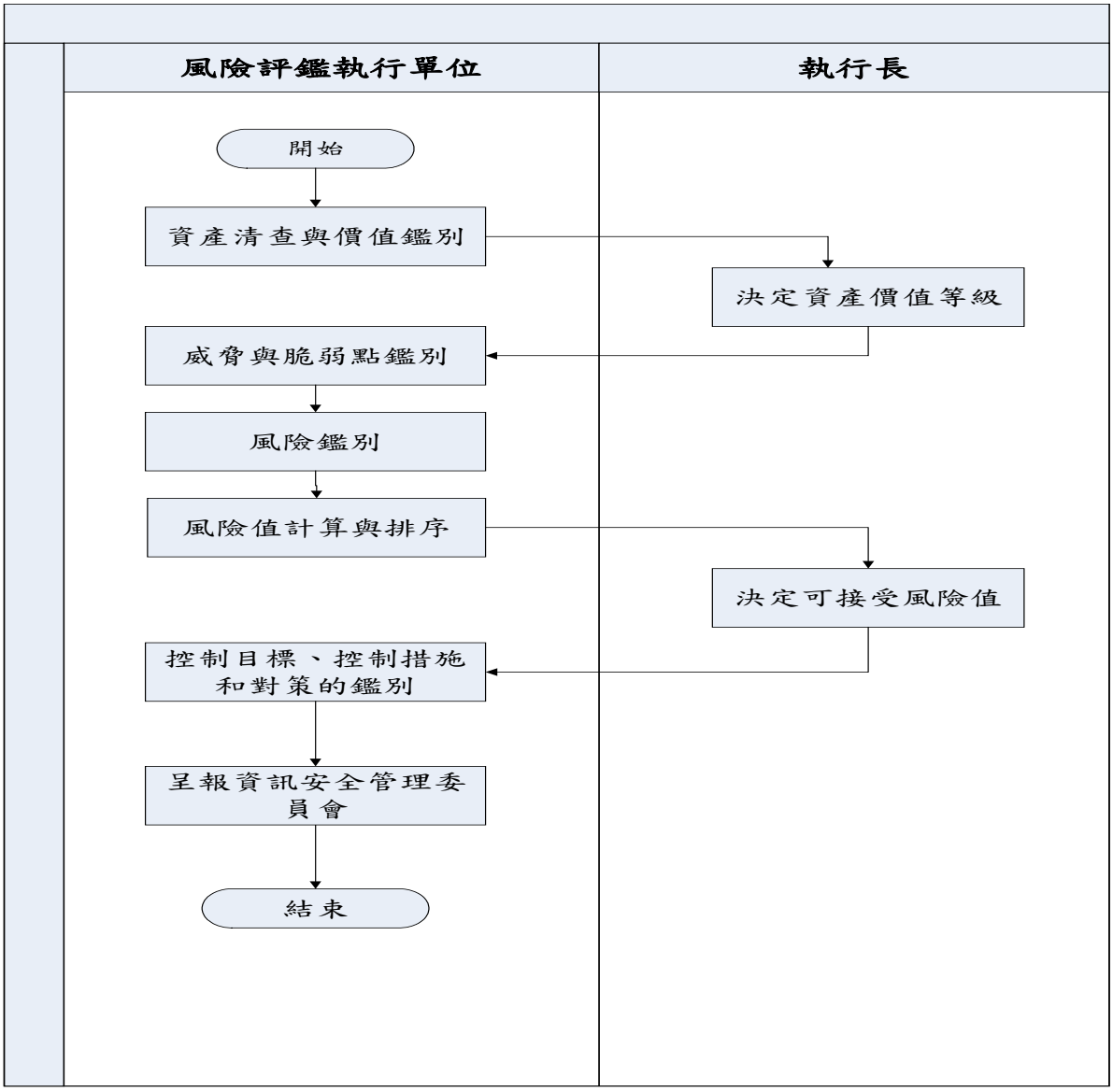


圖 1：風險評鑑流程圖

一、 資產清查與價值鑑別

權責單位應執行資產清查，並依據「資產管理制度作業說明書」所定義將資產分類及編號，並鑑別資產價值。

二、 資產風險評鑑作業

經資產價值評鑑作業所鑑定的高資產價值等級之資產(係指資產價值 4 以上者)，需進行後續風險評鑑作業，挑選威脅與脆弱點，並進行評鑑分數。

(一) 威脅/脆弱點鑑別

評估各資通系統可能面臨的威脅/脆弱點，再依各資產類別列出一般可

能面對的威脅/脆弱點因子後，進行風險分析。相關威脅/脆弱點請參見「風險評鑑表」之風險因子資料庫。

(二) 風險鑑別

風險評鑑決定資通資產之價值、識別存在（或可能存在）的威脅與脆弱性、識別既有之控制措施以及其對已識別風險之效應、決定潛在後果。各項資產依據風險衝擊程度表(如表 1)及風險可能性等級表(如表 2)所定義去評定資產的風險衝擊程度和可能性等級。

表 1：風險衝擊程度表

| 等級 | 風險衝擊程度等級 |
|---|---|
| **1** | 無傷害<br>1.遭受此風險不會造成金額損失<br>2.對組織無任何影響<br>3.組織可以接受 5 天以上服務中斷/資產無法使用 |
| **2** | 輕微傷害<br>1.遭受此風險金額損失可接受<br>2.該風險對組織造成的衝擊可接受<br>3.組織可以接受 3 天以上至 5 天內服務中斷/資產無法使用 |
| **3** | 低度傷害<br>1.遭受此風險金額損失超過十萬元以上<br>2.該風險對組織造成一定程度的衝擊<br>3.資料損毀，組織資料可供回復<br>4.組織可以接受 1 天以上至 3 天內服務中斷/資產無法使用 |
| **4** | 中度傷害<br>1.遭受此風險金額損失超過一百萬元以上<br>2.該風險對組織造成一定程度的衝擊(如平面媒體負面報導)<br>3.資料損毀，組織有備份資料可供回復<br>4.組織可以接受 4 小時以上至 1 天內服務中斷/資產無法使用 |
| **5** | 重大災害<br>1.遭受此風險金額損失超過一千萬元以上<br>2.該風險對組織造成重大的衝擊(如網路/新聞媒體負面報導)<br>3.資料損毀且組織無任何備份資料可供復原<br>4.組織可以接受 4 個小時內服務中斷/資產無法使用 |

表 2：風險可能性等級表

| 等級 | 風險可能性等級 |
|---|---|
| **1** | 年度發生次數為 1 次或未發生 |
| **2** | 年度發生次數為 2 次 |
| **3** | 年度發生次數為 3 次 |
| **4** | 年度發生次數為 4 次 |
| **5** | 年度發生次數為超過 4 次以上 |

(三) 風險值計算

風險值的計算由資產價值等級、衝擊程度等級值及可能性等級值三個因子構成，風險值的範圍為 1～125，以下為其計算方式：

風險值＝資產價值等級＊風險衝擊程度值＊可能性等級值

範例：資訊類(IF)資通資產價值等級為 5，衝擊程度為 3，威脅發生的可能性等級為 2，計算出風險值為 30。

風險評鑑結果，應彙整於「風險評鑑表」。

(四) 風險排序

依據風險值計算的結果由高而低排列風險的次序，高風險的資產應受到優先的保護。

(五) 決定可接受風險值

就風險整體分析而言，參酌資產的特性、業務屬性、維持運作需求的考量、風險值的範圍（依公式為 1～125），以及年度預算及資源的分配狀況，由資安長核定可接受風險值，對於可接受風險值以下之風險項目，將其視為可接受之風險，不進行防護規劃，針對風險值超過可接受風險值之資產所面臨的威脅與脆弱點提出對策與控制。

(六) 控制目標、控制措施和對策的鑑別

對風險值超過可接受風險值之資產所列出的每項風險，依據 ISO 27001 相關的控制目標及控制措施進行鑑別，彙整控制目標及控制措施於「風

險評鑑表」之「風險處理計畫」。

(七) 呈報資通安全管理委員會

針對上述流程執行結果向「資通安全管理委員會」報告；使「資通安全管理委員會」可以清楚地了解各項資產的重要性，進而設定控制目標、控制措施和對策，並給予最高的注意力及保證程度的等級。

三、 監視和審查

(一) 監視

控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，以便於資安長或資通安全管理委員會做定期或不定期地審視。

(二) 持續改善

風險評估是一個持續改善的過程，並非一蹴可幾，必須隨著風險管理的結果，再重新進行評估，以期在風險管理上能不斷地改進，確保資通資產均處於最佳保護之下，提供持續不中斷的營運。

為保持本風險評估方法之有效性與適用性，資通安全推動小組得定期檢討可接受風險值與威脅及弱點評估表之項目。

(三) 風險重新評估

各資通資產風險值之重新評估可分為定期與不定期，每年應至少執行一次風險評估；由權責單位負責於新增系統、系統有重大異動或作業環境改變時執行不定期之風險評估。

當資通資產異動時需進行的部份風險評鑑，將以內容增訂的方式附註於「風險評鑑表」後。另如有涉及風險管理控制措施的新增，亦將以內容增訂的方式附註於「風險評鑑表」之「風險處理計畫」。

## 陸、參考文件

一、 B330-I305 資產管理制度作業說明書

## 柒、使用表單/系統

一、 資訊資產管理系統-資產風險評鑑
二、 資訊資產管理系統-風險處理計畫