SoD 的衝突矩陣

編撰：屏東大學 周國華老師 2026-03-25

在 **AIS (會計資訊系統)** 與 **內控 (Internal Control)** 的領域中，**SoD (Segregation of Duties，職能分工)** 是防範舞弊的核心。

當我們提到 **「SoD 衝突矩陣」(SoD Conflict Matrix)** 時，「矩陣」是一種**二維的交叉比對工具**，用來檢查企業內部的職限（Permissions）是否發生了「自己審核自己」的違規情況。

1. 「矩陣」在 SoD 中的長相

想像一張 Excel 表格，橫列（Rows）和縱欄（Columns）列出的是同一個清單：**「不同的業務職能或系統權限」**。

- **橫列 (Row)：** 員工擁有的權限 A。
- **縱欄 (Column)：** 員工擁有的權限 B。
- **交叉點 (Cell)：** 如果 A 與 B 兩個權限**不應該**由同一個人同時擁有，這個交叉點就會標示為「衝突」(紅色或打叉)。

2. 為什麼要用矩陣？（衝突的視覺化）

矩陣的意義在於**窮舉所有可能的組合**。

在大型 ERP 系統（如 SAP 或 Oracle）中，權限多達上千種，單靠人腦無法判斷。透過矩陣，我們可以定義出哪些組合是「不相容職務」(Incompatible Duties)。

職能 (橫 \ 縱)	建立供應商	批准付款	簽發支票	庫存盤點
建立供應商	—	衝突	衝突	安全
批准付款	衝突	—	衝突	安全
簽發支票	衝突	衝突	—	安全
庫存盤點	安全	安全	安全	—

例子：如果某人在矩陣中同時勾選了「建立供應商」與「批准付款」，這就是一個經典的 SoD 衝

突。他可以編造一個假公司（虛假供應商），然後自己核准付錢給這家公司。

3. 矩陣在審計上的三大功能

A. **預防性控制 (Preventive)：**在幫員工設定系統帳號權限時，先跑一遍矩陣，如果發現衝突，系統就拒絕存取。
B. **偵測性控制 (Detective)：**定期掃描現有的員工權限。有時候員工職務調動，舊權限沒刪掉，新權限又加上去，就會在矩陣中現形（這叫 **權限蔓延 Privilege Creep**）。
C. **風險評級：**矩陣的交叉點可以標註風險等級（高、中、低）。「高風險」衝突（如：採購 + 付款）必須立刻處理。

總結

在 AIS 的實務中，SoD 通常要求將 ARC 三種職能分開：

- **A**uthorization (核准)
- **R**ecording (紀錄/會計)
- **C**ustody (資產保管)

「矩陣」就是一張「不相容職務的對照表」。

它幫助管理者一眼看出：**「如果一個人同時做了 A 事又做了 R 事，會不會導致舞弊三角中的『機會』大增？」**