

出事那天， 你拿得出什麼？

電商品牌個資風險與證據診斷

把看不見的責任風險，變成看得懂、改得動的缺口清單。

服務費

NT\$ 120,000 （未稅）

單一品牌標準診斷固定價／查核範圍於簽約前確認，超出另案估價

平台說「不是我們」，你怎麼辦？

不先判定事故責任；先問自己能拿出什麼紀錄。

假設情境

「我們查過系統，沒有異常。
資料可能是從你們品牌端流出去的。」



你說不是？
那你拿什麼證據反駁？

個資安全有沒有做好？該有的紀錄拿不拿得出來？
還是你以為只要講「我們用的是大平台」，就不會吃罰單？

※ 實際責任仍取決於事實、各自法定義務與主管機關調查結果。

有制度、有執行、能證明有執行，是三回事。

診斷要找出的是這三件事之間的落差。

01

有制度

有規範、流程、
職責與管理要求？

02

有執行

平常真的照做？
人員與外包是否落實？

03

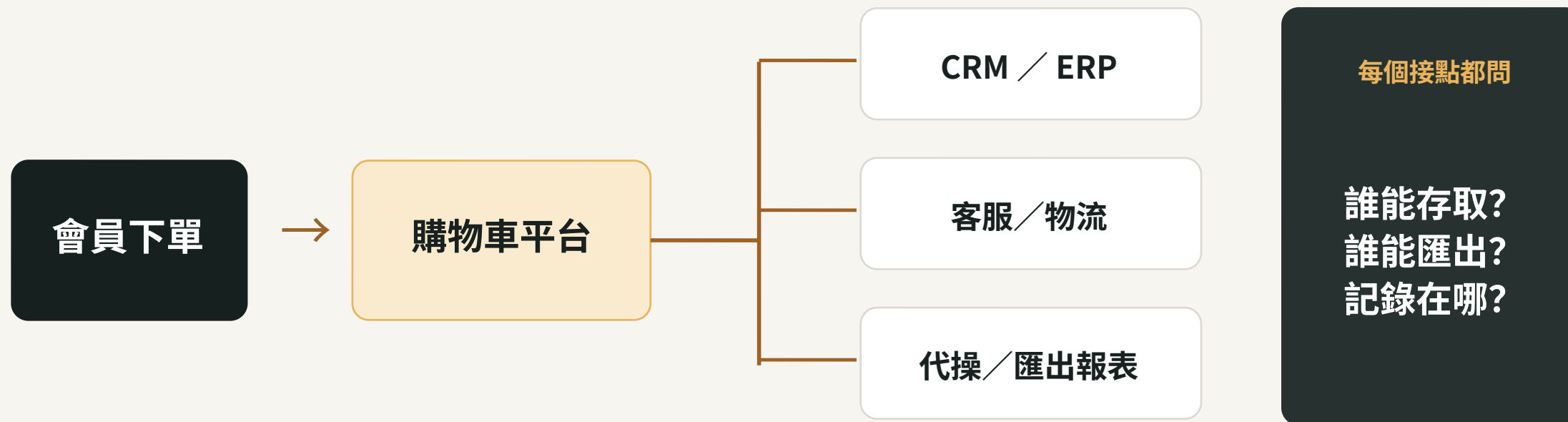
有證據

權限清冊、紀錄、
查核結果拿得出來？

很多人以為買了購物車、寫了 SOP 就算做完。問題是：主管機關真的來查，你拿什麼證明你平常有在做？

會員資料經過誰的手？

以下是常見電商資料接點示意；真正路徑會依你的系統逐一盤點。



資料越會流動，越需要有人知道流向與權限。

五個面向，把缺口一次查清楚。

不是請你重寫每一份文件；是先確認哪些地方沒有被管理。

- | | | |
|----|---------|----------------------|
| 01 | 資料流向 | 會員資料在哪些系統，流向哪些對象？ |
| 02 | 存取與匯出 | 員工、離職人員、委外團隊的權限怎麼管？ |
| 03 | 委外與責任 | 平台、物流、客服、行銷代操，誰負責監督？ |
| 04 | 安全與應變 | 異常怎麼察覺？發現事故怎麼應變與通報？ |
| 05 | 證據與持續改善 | 制度做過嗎？執行軌跡和改善紀錄在哪？ |

最後交付的不只是「這邊有問題」，而是讓你知道先補哪個、誰該補、怎麼補。

結案交付四套檔案，能查、能改、能派工。

不是只告訴你有問題，而是把風險、證據與改善動作整理成可使用的成果。

01 會員資料流向圖

系統、資料類型、權限與委外接點
PDF + 可編輯圖檔

02 風險缺口清單

位置、判斷依據、等級與負責窗口
Excel 可篩選明細

03 查核證據盤點表

既有紀錄、缺失、來源與可取得狀態
Excel 證據索引

04 改善路線與預算

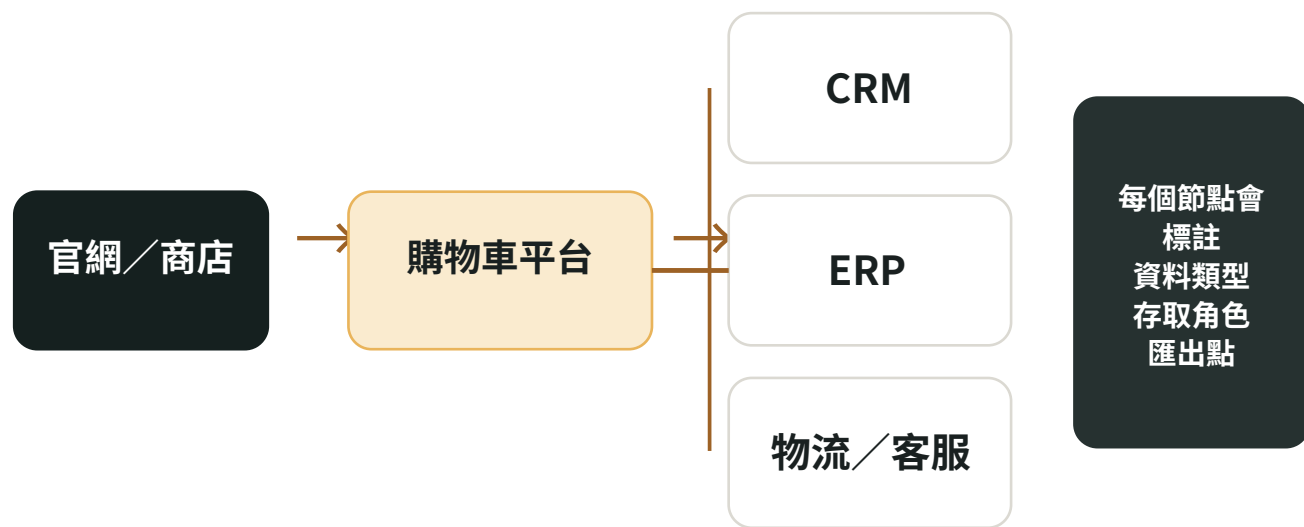
優先順序、負責人、預估時程與成本
Excel + 管理摘要 PDF

另附：一頁管理層決策摘要 + 一次結案說明；沒查到的紀錄不會代你補造。

會員資料流向圖 | 先搞清楚資料到底流去哪裡。

交付重點不是畫得漂亮，而是讓你一眼看懂哪些系統、哪些人、哪些委外會碰到資料。

交付 01



你會看到什麼？

- 哪些系統會碰到會員資料
- 哪些外包／平台／人員能接觸
- 哪裡有匯出、同步與 API 接點
- 哪些地方目前根本沒人說得清

交付格式：PDF + 可編輯圖檔（方便後續補充與派工）

風險缺口清單 | 把問題變成可以追的工單。

不只寫「這裡有問題」，而是直接標出位置、依據、優先級與建議責任人。

交付 02

缺口項目	位置／系統	判斷依據	等級	責任窗口	建議下一步
離職帳號未停權	CRM	帳號清冊與登入記錄比對	高	IT／HR	停權、補權限複核流程
委外匯出未留痕	報表匯出	有委外作業，無核准紀錄	高	營運	限制匯出並建立簽核
事故通報只有 SOP	管理制度	有文件，無演練紀錄	中	管理部	安排演練與改善追蹤
客服權限共用	客服系統	多人共用帳密，無個人辨識	中	客服主管	改個人帳號並保留存取紀錄

交付格式：Excel 可篩選明細，可直接拿去開會、派工、追蹤。

查核證據盤點表 | 哪些東西拿得出來，哪些根本沒有。

主管機關真的來問時，至少要先知道手上有什麼、缺什麼、還能不能補。

交付 03

檢核項目	現有證據	狀態	來源／保管處	補件建議
權限清冊	2026 Q3 帳號名單	已有	IT 共用資料夾	補最近一次複核紀錄
離職停權紀錄	無法提供	缺失	—	建立停權單與保存軌跡
委外保密／委任文件	合作合約 2 份	部分	法務資料夾	補委外資安要求條款
事故應變演練	未實施	缺失	—	排定一次演練並留紀錄

交付格式： Excel 證據索引，可直接當查核準備清單；找不到的紀錄會如實標示缺失。

改善路線與預算 | 先修哪個、誰來修、要花多少。

讓老闆知道順序，讓執行人知道下一步。

交付 04

立即處理（7 天內）

- 停用高風險帳號
- 限制委外匯出權限
- 保存現有證據快照

預估成本：低～中

短期改善（30 天）

- 補制度缺口
- 補簽核與權限複核
- 建立事故回報流程

預估成本：中

中期工程（60-90 天）

- 系統權限重整
- 串接紀錄機制
- 教育訓練與演練

預估成本：中～高

最後會附一頁管理摘要，方便你決策：「哪些先做、哪些另案、哪些可以延後」。

3-4 週，完成一次有邊界的診斷。

時程為預估；依企業提供文件、訪談及帳號存取配合程度調整。

01

啟動週

範圍確認

確認品牌、站點、系統清單
與委外關係；取得聯絡窗口

02

第 1-3 週

抽樣查核

文件檢視、流程訪談、
權限及執行證據抽核

03

第 3-4 週

報告交付

提交四份成果、管理層說明、
界定下一步改善工作

不需要交出整份會員資料：原則上用遮蔽畫面、權限清冊與必要的流程紀錄進行確認。

診斷就是診斷；改善工程另行立案。

12 萬固定費用以事前確認的範圍為準；新增系統、委外對象或擴大抽查，另行估價。

本階段包含

- ✓ 系統、流程、委外關係盤點
- ✓ 證據與制度落差抽核
- ✓ 風險分級與改善先後順序
- ✓ 四份交付成果＋一次說明會

以下另案計費

- 系統程式修改、權限重建工程
- 滲透測試、事故鑑識與緊急應變
- 法律意見、裁處救濟或訴訟
- 長期代管、持續稽核與新系統評估

不承諾「零風險、保證合規、一定免罰」；依法調查與裁罰結果不由顧問決定。

先把問題查清楚， 後面的工程才不會亂做。

確認服務範圍只需要三樣資訊：

- 01 正在使用的購物車、CRM、ERP 等系統
- 02 接觸會員資料的合作廠商與外包單位
- 03 現有制度、權限及紀錄（有多少就提供多少）

範圍確認 → 12 萬固定費用 → 保密／委任 → 啟動診斷