論述》管理 · 資訊

從運動彩券舞弊案看資訊系統的內控作為

前近爆發的運動彩券監守自盜案，即為資訊作業內控失靈的負面教材。人是工作的主體，理應是內控對象之一。惟有制度落實成習，佐以稽核管理活動，內控規範始能見其竿影。

黃芳川（行政院主計處電子處理資料中心研究訓練組組長）

壹、前言

最近，『電腦會揀土豆』的廣告又出現在電視，顯見大眾對於電腦作業的信賴。

基本上，一個電腦資訊系統在資料輸入 (input) 與結果輸出（output）之間的處理運算過程 (process)，恰是一個「黑箱」。它必須經過系統分析師的流程規劃、程式設計員的程式編寫、專案管理者的品質監督管理、系統人員的一再測試驗證、資料管理者的資料輸入與操作、系統維護者的異常發現與修正、資安人員的安全檢視、稽核人員的稽核活動等，各環節角色各盡其職，共同建立百分之百的正確性與可信度，才使得這個「黑箱」贏得使用者的信賴。選舉計票系統就是一個典型實例。

從有資訊系統以來，就存在有資訊處理的安全管理規範；時下正夯的資訊安全管理、內部控制管理、永續營運等議題係由其衍伸而來。主要目的就是在防止資訊流程內各環節角色與來自網路的人為無意或蓄意破壞與犯罪，以導引組織內所有成員均能落實相關安全處理行為，進而塑造一個永續、專業、績效與可信賴的組織形象。依此，內部控管與資安管理目標不謀而合。

任何業務工作過程都存在可控制和不可控制的風險，管控的目的是將風險降至可以接受的範圍；資訊系統亦然，其風險的大類有：(1) 天然災害，如地震、水災；(2) 軟體設計瑕疵，如流程疏漏、權限不當；(3) 非故意的操作錯誤，如誤植資料、參數設定失當；(4) 人為的犯意破壞，如駭客入侵、監守自盜等。依據相關統計，6 成 5 來自員工非故意的錯誤，其次是天然災害，接著才是人為的蓄意破壞或犯罪。總而言之，人員才是資訊風險管理的主要課題，內部管控機制則是構築

這個課題的第一道防線。

貳、資訊系統的內控作為

拆解資訊業務發展的工作流程，大致分爲：系統分析、程式設計、測試、建置上線、技轉訓練、既有資料檔 (庫) 轉置、新增資料鍵入、整體資料之處理 (含查詢、更新、刪除、輸出)、系統功能之變更 (含新增、修改)、系統效能調校、預防性稽查、系統問題之管理與追蹤等環節，其所涉人員應有的作業安全管控基本措施提要如下：

管控目標	相　關　措　施
人員管理	1. 對人員之進用及調派，應作適當之安全評估，對人員之調動、離退，應立即取消其各項識別碼、通行碼。對員工品德、行為、家庭狀況等應適時了解。 2. 對於可存取機敏性資訊或系統之員工，以及配賦有系統存取特別權限之員工應妥適分工，分散權責、實施人員輪調、建立人力備援制度、落實稽核作為。 3. 制定員工私人資訊設備的安全控管程序規定。 4. 制定委外廠商安全管理規範。
系統發展	1. 應用系統在規劃分析時應將安全需求納入考量，開發、測試與正式作業應分別使用不同帳號在測試與正式環境主機。尤其對於程式編碼 (coding) 與系統交付後的執行，應分由不同人員負責，並重設權限密碼；指定專人管理應用程式原始碼、資料庫及執行檔。 2. 委外開發合約需規範智財權之歸屬、程式原碼提供與變更後的即時更新。 3. 系統上線前需作弱點掃描及程式碼檢查 (core review)。
系統測試	落實白箱測試（功能邏輯性測試）、黑箱測試（資料正確性測試）、虛擬資料測試、平行作業測試等措施。
資料存取	1. 對於線上輸入資料，應建立防呆功能與第二層線上審核確認機制。 2. 重要資料應有重複輸入 (double keyin) 驗證、鍵入資料總數核對。 3. 各應用系統應訂有存取權限管理機制，及忘記密碼之處理應落實身份確認程序。定期檢視使用者存取記錄。 4. 訂定密碼、長度及文數字符號組成之相關規定。一定時間內未操作的安全保護機制。

管控目標	相　關　措　施
服務品質	1. 訂定系統服務水準，每月彙報系統服務水準統計報告。 2. 定期系統容量規劃、系統效能檢視與調校、UPS 不斷電設備、AVR 穩壓器等設備管理。
異動管理	1. 制定異動管理，涵蓋人員及軟硬設備的變更。 2. 對於系統變更應建立安全標準作業流程。 3. 各工作環節均應有備份人力參與。 4. 人員異動應至少有一週交接期，及交接清單。
機房安全	1. 實施門禁、環境溫控火災防護、物品出入等管理，並專人檢視報表。 2. 應訂定電腦系統之災害應變與回復計畫，包括異常事件通報、. 建立定期備份機制及辦理回復演練。
通訊及操作	1. 機敏資訊之網路傳輸應採取加密、授權認證等措施，並指定專人保管、存取、發送、複核、記錄等處理。 2. 業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作應分由不同的人員執行。
個資保護	1. 制定私密性與機密性資料處理管理規定。 2. 重要報表密封、親自交付簽收。 3. 訂有儲存體報廢或移他使用時的消磁程序，並指定專人處理。
稽核管理	建立內控管理稽核制度，定期辦理稽核活動。

參、現有資訊管控的隱憂與因應

由於資訊技術的提升、使用者功能需求量增質高、系統整合殷切、委外策略風行、網路技術應用竄升、資訊安全層次高築等諸多因素交相激盪之下，衍生時下資訊管理隱憂。

(一) 一人多角色鬆綁了管控嚴密性：或限於人力規模、組織大小、經費多寡、工作慣性惰性等因素，資訊單位衡量輕重之下，或多或少都將部分管控措施聊備一格，與風險豪賭一番。一人兼任多角色，球員兼裁判，衍生控管漏洞。是以，釐清角色權責，加強權限控管與落實稽核，是爲正道。

(二) 委外制度下的安全管控只寄望在一紙保證書：

不僅系統開發，甚至於操作、維運、資料處理、人力...等工作皆大肆委外，而委外人力與系統的安全管理卻僅交付予一紙安全保證書或契約書。於是，偷改考試分數、洩題舞弊、個資竊賣...等情事發生屢見不鮮。在委外有理的大環境下，惟有資訊單位同仁必須在專案監督管理方面多所著墨，落實權責，始能提高安全管控係數。否則，任何管控機制都是一堆文件。

(三) 內控機制落實僅適用於下層同仁：個人資訊已成爲流通的商品，促使網路成爲人性貪婪速成的歧途。由於數位資訊已成不可回頭的事實，各機關或單位多所推動資訊安全管理機制導入之認證、複核。但如果「銀子花了，習慣照舊」，那該如何是好？最直接的落實方法是自上而下，一視同仁，切莫有特殊例外，何況主管都被賦予較高或最高的資料存取權限，而管理同仁礙於位階，遇此常以權宜方式處理，實屬高風險群，宜愼之。

(四) 以爲科技是管理的萬靈丹：從人性可以看見科技的漏洞，反之則不然。過度重視凡事以科技流程解決問題，而輕忽人性面管理，將導致時間一久弊病就現。在科技運用之餘，效率與效能皆可提升應是肯定的，但管理者工作量相對增加，如果此時以爲組織架構可以更加扁平化，那麼管理品質降低或過勞問題浮現，也就不足爲奇了。

肆、結論

前近爆發的運動彩券監守自盜案，即爲資訊作業內控失靈的負面教材，北富銀眞是賠了夫人又折兵。人是工作的主體，人性如流水，清醒時一湖秋波，醉迷時滔天巨浪。管理學與人性學雷同，皆有性善與性惡之主張；但兩學派殊途同歸，都是從人性深底黑洞的風險防範爲基點。這也是內控一再被揭示警醒的原因。

快速、正確是資訊作業特性。因爲快速，帶來效率；因爲正確，帶來信任。資訊作業內控的措施，就是在規劃、開發、執行、維護等工作流程中，從上到下全員落實管理規範，確保系統使用者信賴目標的達成，也藉以杜絕個人非分妄想。

『窮則變，變則通，通則久，久則倦，倦則殆，殆則窮』是萬事消長循環的道理，一個制度亦然。要想破除五分鐘熱度的魔咒，就須佐以稽核管理活動，以提醒使用者隨時隨地遵循內控規範。

管理實務一句箴言，『可用設備管理的就不用人力，設備不能管理的就用制度來管理』。組織階層有高低，同事關係有親疏，以制度當作管理的共同規範，才不致於發生因人而異的管理脫軌行徑，予人可乘之機。惟有制度落實成習，內控規範始能見其竿影。❖