資安稽核常見問題

◎黃小玲

前　言

資安稽核時常發生問題，有時是稽核人員的疏失，有時是受稽單位的準備不足，更或有時是「莫非定律」光臨，所有問題一起出現在同一個時間點。

前陣子速食業者油品稽核事件，鬧得沸沸揚揚，從一開始的速食業者用油到底多久換一次、油品更換紀錄造假事件、發現速食業者滅火器逾時 8 年，到最後議論麵包適當保存期限是多久？究竟，稽核可否界定範圍？符合國家規定等不等同符合消保官的稽核準則，以及稽核人員的標準與受稽單位的觀點如何一致？

以上這些問題，就從一個小小的稽核開始。資安稽核也是稽核的一種，從這個事件來看幾件資安稽核可以借鏡的地方。

壹、天上掉下來的禮物要不要接？

在上述油品稽核事件中，滅火器應該不在消保官的稽核計畫中，但是當發現這樣的缺失時，要不要寫入稽核缺失表內？要不要繼續追蹤改善與否？新聞沒有進一步的報導。若這樣的缺失發生在資安稽核情境中，稽核人員若見獵心喜，決定改變方向往消防檢查方向前進，如此一來可能延誤或只得變更其他稽核行程以繼續追查。稽核的評估重點是在已事先定義好的稽核範圍內，稽核重點若在油品逾時不換，則應確保過程不致失焦；滅火器過期，則列入稽核註記，下次稽核時再加強檢視或是交付不同單位列入考核重點。

稽核技巧：稽核首重規劃，縱有天上掉下來的禮物，稽核人員還是應該著重在原有規劃之稽核目標與行程上。

貳、稽核員永遠是對的？

稽核場景一：稽核人員對著機房管理人員露出想一探究竟的表情說：這個機房每日檢查表（包括機房溫濕度、系統及環境異常等）內的筆跡與墨色都一樣，且數月來都是填寫「OK」，而且連明天的紀錄都已填寫，我懷疑資料是不是造假？機房管理人員不置可否：每天都是我填寫，筆跡與墨色當然都一樣，至於明天的紀錄是不小心填太快，只是一時疏忽。

稽核技巧：稽核員可以假設自己像名偵探柯南，但偵探可以推理，稽核則講求客觀性證據。因此，稽核員不應自行判斷這個紀錄表是造假的，擅自認爲這樣的狀況一定是不實紀錄。稽核若沒有證據顯示異常或不符合，則不能憑藉著稽核人員的天縱英明而完成稽核報告。

參、世界上最遠的距離

稽核場景二：稽核員在稽核會議上報告今日的稽核時程後，發現會議室內的受稽單位代表紛紛露出詭異的笑容。稽核員順利完成早上 9:30 至 10:30 的稽核行程，準備前往下一個辦公場所進行接下來一小時的稽核。陪同人員這時才悄悄

地跟稽核人員說：不過我們另一個稽核場所來回要一個半小時哦！稽核人員這時才頓悟，稽核最遠的距離不在你跟我之間，而在受稽核單位明知來回要一個半小時，卻事先不告訴你。

稽核技巧：稽核人員與受稽單位應仔細確認稽核計畫內的所有規劃，包括範圍、業務複雜度與時間的安排是否妥適等。

肆、全部都是機密，通通不許看

稽核場景三：稽核員看著防火牆管理者說：我想看看你所負責的防火牆服務埠開?的申請表格。管理者頻頻搖著頭說：這類的申請表格，我們內部列爲機密，不好意思，如果沒有正式經過申請審核，我無法提供。稽核員莫可奈何地說：好吧，那可不可以讓我看一下你針對防火牆所做的風險評估報告。防火牆管理者說：抱歉，那也是機密文件！

稽核技巧：通常在資安稽核開始時，會要求稽核員簽署所謂的保密切結書。基於保密切結的情況下，如果內容真是涉及機密，受稽單位當然可以拒?。但稽核員若只想檢視處理機密資訊的過程，倘仍一味地拒?，則稽核也無從判斷資安防護程序的嚴謹度。其實利用保密切結的簽定或部分內容遮蔽的技巧，即可顧及機敏資訊不外洩，又可收稽核之效。

伍、人員跟你玩躲貓貓時，怎麼辦？

稽核場景四：稽核順利開始，每位稽核員都有 2 至 3 位受稽人員待命，準備接受實地檢閱或文件紀錄的對應。很快地，稽核員發現他前面一個人都沒有，剛剛一片熱絡的情況，瞬間不復見。稽核員想想：他剛請第一位受稽人員去拿一分管理文件，因爲沒回來，所以只好轉換稽核項目，請第二位負責人去拿系統帳號申請紀錄；第三位受稽人員，好像是說他所負責的資安教育訓練需要會辦人事室，所以需要去人事室拿紀錄過來。問題是：怎麼三個人都一去不回呢？距離第一個人離開的時間至少 20 分鐘了吧！終於第一個人回來了，上氣不接下氣地說：對不起，請問你剛剛的稽核問題是什麼？我們系統管理者不確定你要的是那份管理文件？

稽核技巧：首先，稽核人員必須了解維持稽核計畫可以確保稽核品質，但稽核時的情境題，千奇百怪，如果只是墨守成規或不懂得變通，則稽核效果有限。第二個問題是，如果受稽人員真的不懂得稽核員在問什麼問題時，務必要問清楚，才不會造成雙方認知的差距。

陸、Hands on or Hands off（接手或不插手）

稽核場景五：稽核員看著 AD Server(目錄伺服器)的系統管理員說：我想看一下單位內的帳號與密碼安全性設定原則。管理者慌亂地說：自從上位管理者離職後，我都沒改變設定。繼之，他不熟練地操作著，努力想秀出稽核員所要看的系統設定畫面。努力一陣後，他看著稽核員說：可不可以由你操作比較快？稽核員想想有道理，接手將滑鼠點了幾下，果然很快找到設定的畫面。就在此時，突然有人走進機房叫喊著：同仁紛紛反應電子郵件出現錯誤訊息，無法正常收發 e-mail，也有人反應無法登入網域。管理者與稽核員面面相覷地互喊：不是我！

稽核技巧：稽核員不論多麼熟悉所稽核之系統，都應避免直接接觸線上系統，以免發生干擾正常維運的狀況。

柒、稽核證據像魔術一樣消失時

稽核場景六：一天的稽核終於結束，到了結束會議。稽核人員一一報告今日的稽核缺失時，突然技術部門主管開口：不好意思，因爲我昨天才發 mail 請我部門所有人員注意合法軟體的問題，您真的在我部門發現有同仁的軟體版權有逾期的問題？可不可以請問是我部門那個同仁？稽核員被如此一問，有點愣住：我記得應該是坐在三樓入口右手邊那位先生。技術主管疑問：可否再明確一點呢？或是等一下我們一起前往那位同仁位置上看一下？

稽核技巧：對稽核人員最糟糕的可能情境之一是：稽核證據在轉身時就消失。上述事件稽核人員當然可以再次前往現場進行稽核確認，不過很可能的狀況會是：非授權軟體早已被移除乾淨。如何確保稽核證據不會像泡沫般消失，除了稽核陪同人員的見證外，稽核人員應紀錄所有稽核發現的人、事、時、地、物，並將所有違反事項詳實記載於工作底稿內，如此皆有助於稽核證據的再次真實呈現。

捌、結論

學習稽核應對概念與技巧，對稽核人員與受稽單位都一樣重要。通俗地說，稽核是稽核人員與受稽單位某種競智的表現。但是最佳稽核情境應該是雙方基於互信互利的基礎，對事件稽核的準備與過程中，皆依計畫進行，其所產出的獨立性稽核報告能得到受稽核單位的認可，彼此遵守稽核規範與準則，則可大幅避免出現資安稽核的謬失。

（作者爲國家資通安全會報技術服務中心組長）