清流月刊中華民國九十八年八月號

如何讓資安稽核發揮最大的效益，而非淪為管理制度文件的陳列，是機關在規劃資安稽核時應先列入討論的議題。

如何規劃機關資安稽核

◎ 黃小玲

壹、前言

某機關業務部門資安承辦人員匆忙走進資訊室辦公室嚷著：糟糕了！聽說這次年度稽核主管上層屬意由我們來接受稽核。

部門主管聽到心中不禁一顫：上次稽核結果不盡理想，這次一定要雪恥成功。從現在起，所有IT（Information Technology，資訊技術）人員跟相關業務承辦人每天加班，務必將所有資訊安全管理系統的文件全部準備好，而且要求廠商派人駐點協助。

於是所有人日以繼夜地加班數月，稽核的日子終於到來。當天所有IT人員停止休假，廠商也駐點待命。稽核人員浩浩蕩蕩來到時，現場一片肅殺氣氛，文件與紀錄一字排開超過數尺。經過一整天稽核後，單位人員與廠商累壞了，有人開始感嘆，這就是資安稽核嗎？準備一堆管理制度文件？稽核前要加班進行紀錄補單？

以上故事，為某組織真實實錄。

雖然是一個小故事，但資安稽核帶給機關省思的是：為何機關要做資安稽核，目的何在？當然一個可能的原因是，因為政府機關必須配合國家資通訊安全發展方案，那麼就應該準備資安稽核或自我檢視資安執行情形。較積極的回應是：內部因應業務持續，應規劃資安稽核以找出機關可能的風險，並確切定義資安稽核所欲達成之稽核目標。

壹、稽核準備

一、稽核的種類

在進行稽核準備之前應先清楚要執行的稽核種類是第一方、第二方或第三方稽核。第一方稽核為內部稽核，稽核人員通常為內部人員。第一方稽核的準則是稽核員不應該稽核本身的工作，因此在機關內常常面臨的問題是內部沒有足夠的稽核人員，建議可以運用交叉稽核，互相交叉稽核同單位的管理與執行內容；第二方稽核為主管機關對下屬或同儕機關間互相稽核，好處是主管機關對下屬機關的業務熟悉，又可站在督導與管理的角度上進行客觀了解；第三方稽核通常是屬於驗證稽核，由稽核公司驗證機關所建置之資訊安全管理系統是否符合國際標準之要求。

二、稽核的目的

一般稽核的定義：以有系統的過程，所有針對某項特定活動所進行之獨立調查均可稱為稽核。資安稽核的定義則為就所有資通訊實務作業，由稽核人員定期對機關之資訊安全管理，包括資訊資產管理、人員安全、實體安全、網路安全及系統安全等整體安全進行查核，並評估其與資安要求或標準相符合的程度，同時將稽核結果呈報管理階層。配合政策執行資安檢視，原本無可厚非，但機關管理階層應該思考資安稽核的定義與定位後，決定稽核目標是否著眼在發現現有資訊作業相關之風險，提出改善建議後，確保機關業務之持續性。

三、稽核的範圍－誰應該被稽核

定義資安稽核範圍時，可以先討論一個議題－資訊安全工作是由誰或內部那個單位負責？因為資訊化時代的來臨，幾乎所有業務都透過電腦進行作業，而電腦系統的建置與維護又是由資訊部門負責，因此可看到機關的資安聯絡人幾乎都是資訊處室的人員。從以上觀察得到的結論是：既然電腦是資訊人員負責，當然資訊安全也應該是他們規劃，那麼稽核的範圍當然是以資訊部門為主！不過這是正確的嗎？資安稽核是資訊人員的業務，其實是一種迷思。資安稽核應著眼於評估機關重要業務，分析可能風險所在，試著找出機關存在之資訊弱點與可能發生的風險後，提出建議對策供機關參考，所以確認稽核範圍與稽核目標應為機關規劃稽核的首要動作。

四、稽核的依據

機關除確認稽核時程規劃外，亦應先定義稽核時的依據，依據何種的資訊安全要求與機關內要求的遵循與符合性。現行政府機關的資安稽核依據有以下兩種：

（一）ISO 27001的國際資訊安全標準

此為現行國際資訊安全標準，亦為資訊安全管理系統（ISMS）的驗證標準，於第三方稽核時使用此稽核依據。

ISO 27001: 2005
4 Information security management system資訊安全管理系統 5 Management responsibility管理階層責任 6 Internal ISMS audits內部ISMS稽核 7 Management review of the ISMS 管理階層審查 8 ISMS improvement 資訊安全管理系統改善
Annex A附錄A Control objectives and controls控制目標與項目 A.5 Security policy 資訊安全政策 A.6 Organization of information security 資訊安全組織 A.7 Asset management 資產管理 A.8 Human resources security 人力資源安全 A.9 Physical and environmental security 實體與環境安全 A.10 Communication and operation security 通訊與作業安全 A.11 Access control 存取控制 A.12 Information systems acquisition, development and maintenance 資訊系統獲取、開發及維護 A.13 Informaiton security incident management 資訊安全事故管理 A.14 Business continuity management 業務持續管理 A.15 Compliance 遵循性
資料來源：ISO 27001:2005，本表自行整理

表1 ISO27001稽核條文

（二）資通安全外部稽核(自我評審)表

依據「國家資通訊安全發展方案（98年至101年）」第6、7項行動方案「推動資安治理」及「推動資訊與資訊系統分類分級」辦理，所訂定的「政府機關（構）資訊安全責任等級分級作業施行計畫」規範中定義，除希望政府機關能遵守行政院及所屬各機關資訊安全管理規範外，各機關應依其不同資安等級規劃稽核方式如下：

1. A級單位每年至少執行2次內部稽核。
2. B級單位每年至少執行1次內部稽核。
3. C與D級單位得執行自我檢視。

以上所提之稽核工作事項的依據，以行政院資通安全稽核服務團的資通安全外部稽核（自我評審）表為主，查核項目大致上同ISO 27001分類，係參照ISO 27002的最佳實作規範，並條列稽核的檢視重點。

五、資安稽核人員資格與所需的技術要求

機關所挑選之稽核員除應確認稽核目標外，並須確保整個稽核之公平程序，同時誠如前言提及的稽核實景，稽核不單是看文件數量的多寡，亦應藉由稽核過程了解機關內的資訊安全管理系統是否有效地建置與被維護著。因此，機關在遴選稽核員時，除了要有稽核員的證照外，稽核經驗更是不可或缺的要求。稽核人員能力要求，應包括稽核規劃能力、稽核實務作業能力及報告撰寫編製能力等等。資訊安全管理系統雖然號稱是一個管理系統，但此系統是架構在資訊作業環境下，所以資訊技術的專業領域與觀念為資安稽核所必要之知識，如：資訊系統網路通訊技術(網際網路、區域網路等)、資訊系統技術(作業系統、應用系統與資料庫等)，及資訊安全防護技術(防火牆、入侵防護系統與惡意軟體防範等)。

貳、稽核程序

一、稽核流程

依據圖1，分解出機關資安稽核的規劃程序。在確認稽核目的與範圍後，下一次則是確認稽核方法；稽核方法計有：觀察法、訪談法、實地檢閱法－主要以抽樣法為主、邏輯驗證法。

稽核程序書面化，包括稽核計畫應事先送達受稽單位，以確認雙方有共同認知與流程，且針對不適合之稽核計畫可以提前討論並解決。稽核員亦應準備工作底稿，詳細列出稽核項目，依稽核計畫所規劃之時間完成。

稽核講求客觀性證據與紀錄的佐證，過程中所有稽核發現與紀錄應列於工作底稿中。

二、稽核報告

如何給予有效性的建議而非一些吹毛求疵的主觀性意見，為稽核員產出客觀性稽核報告的主要課題。稽核報告除針對管理優異處給予受稽核單位肯定外，主要是評估受稽核單位資訊安全管理制度之有效性。

稽核報告產出後，必須提報給管理階層，以剖析現行的完善性。稽核程序最後且持續的關鍵步驟是追蹤改善結果，才可以確保機關內所有不可接受之風險皆已妥善處理，並持續維護一個運作良好的資訊安全管理系統。

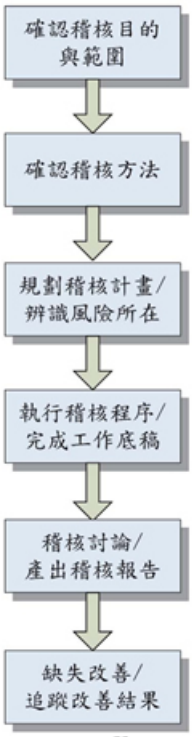

圖1 稽核程序圖，自行整理

參、結論

資安稽核對於機關是必要的工作事項，但如何讓資安稽核發揮最大的效益，而非淪為管理制度文件的陳列，是機關在規劃資安稽核時應先列入討論的議題。當資安稽核開始流於形式、每年的稽核缺失結果都大同小異，而或是機關存在著頭痛醫頭、腳痛醫腳的症狀時，機關應開始細細思量是那個環節出了問題。如果可以定期執行稽核規劃、定義稽核頻率及分析稽核結果時，才不致於發生換了稽核人員或單位，稽核缺失就如雨後春筍般紛紛冒出的情況。

肆、參考文獻

1. ISO 27001: 2005
2. 行政院及所屬各機關資訊安全管理規範，民國88年11月16日行政院研考會(88)會訊字第 05787號函頒。
3. 政府機關(構)資訊安全責任等級分級作業施行計畫，行政院國家資通安全會報98年6月1日資安發字第0980100328號函

（作者為國家資通安全會報技術服務中心組長）

▲Top

清流月刊中華民國九十八年八月號

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。

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，擅自認為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放的申請表格。管理者頻頻搖著頭說：這類的申請表格，我們內部列為機密，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，因為沒回來，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，因為我昨天才發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。

（作者為國家資通安全會報技術服務中心組長）

▲Top