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，爲某組織真實實錄。

雖然是一個小故事，但資安稽核帶給機關省思的是：爲何機關要做資安稽核，目的何在？當然一個可能的原因是，因爲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。第一方稽核爲內部稽核，稽核人員通常爲內部人員。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；第二方稽核爲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爲稽核。資安稽核的定義則爲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？因爲資訊化時代的來臨，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爲主！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爲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

此爲現行國際資訊安全標準，亦爲資訊安全管理系統（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）表爲主，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爲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－主要以抽樣法爲主、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。

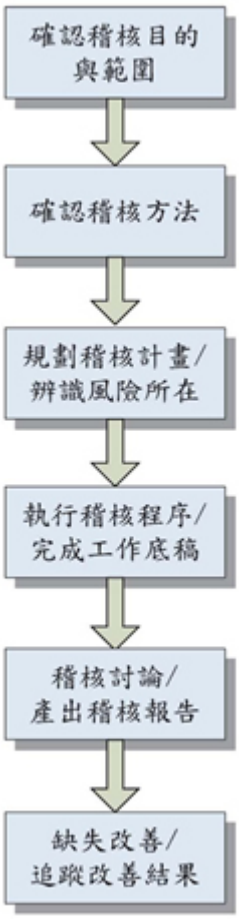

圖 1 稽核程序圖，自行整理

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，爲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。

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，而非淪爲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

（作者爲國家資通安全會報技術服務中心組長）