從稽核到資安管理：視角轉換的 CISM 之路

林煒傑

CISA, CISM, JCCP

現任金融周邊行業｜內部稽核

中華民國電腦稽核協會 專業發展委員會｜委員

前言

自從取得 CISA 國際電腦稽核師認證後，持續為公司執行內部稽核工作，其中電腦稽核更是每個專案必備的領域，小至帳號、密碼分持議題、權限分配合理性、功能是否符合業務需求等，大至公司政策與執行層面是否一致、資安管理機制是否落實並具備持續且有效的監督機制。資訊科技及資訊安全的範疇有多大，電腦稽核涵蓋的面向就有多廣，即使通過 CISA 的洗禮與考驗，僅代表掌握電腦稽核的基本知識與概念，若希望達到融會貫通、游刃有餘的境界，除了累積實務經驗以外，亦須知己知彼，才能為身處不同立場的雙方創造共贏。

稽核人轉化為資安管理者

從業約 8 年至今，為不同機構擔任內部稽核的角色，已經習慣用稽核的思維看待部門、人員及作業流程，雖然以相對客觀的角色檢視各個部門的作業流程，最大的優勢是發現作業流程中的管理誤區與盲點，透過查核點出問題，確實能促使受查單位重新檢視並予以改善。即使猶如上帝視角，在已發生的事實中反覆推論及評估，固然能得出看似合理的結論，卻不如親自走進部門，體會某些查核發現，究竟是導因於人員訓練不足，還是源自於資安管理背後為了權衡風險與成本所做的決定。

基於好奇心，也希望透過換位思考，發掘身為資安管理人在面對資安議題時的考量，與稽核的視角究竟有何差異，於是啟動 CISM 國際資訊安全經理人認證計畫。起初先從 ISACA 官方網站查找 Exam Candidate Guide 初步了解考試科目及範圍，因有先前準備 CISA 的經驗，這次面對同樣 ISACA 認證，採取相似的準備方法：

1. 報名中華民國電腦稽核協會（CAA）認證班
2. 購買 ISACA 官方的 **CISM Questions, Answers & Explanations Database**

3. 制定及落實讀書計畫，以及刻意練習不熟悉的章節及觀念
4. 第 2 點的練習題在考前正確率達 90%以上

CISM 涵蓋領域與 CISA 很相似，最大的不同在於 CISM 是站在資安經理人的角度看待資訊安全；CISA 則是以稽核的角度。例如：

1. 某系統因老舊無法導入多因子認證（MFA），資安經理人會先評估風險及因應成本，規劃補償性控制，並設法將風險降至可接受水準；稽核則是知悉事實後，確認補償性控制之存在性及有效性，評估程序正當性及剩餘風險後，再提出改善建議。
2. 以弱點掃描為例，資安經理人從範圍評估、決定掃描工具、服務水準協議（SLA）到後續修補流程及人員配置等皆需納入規劃；稽核則是依規定檢視掃描範圍、頻率、修補紀錄及例外處理是否合規以及有效落實。

從兩個例子可以看出，資安經理人需要評估資安要做到什麼程度、措施落地後風險能否降至可接受水準、優先順序、如何落地；稽核看的是事實與要求有無脫鉤，設計面與執行面存在差異的原因是什麼？控制點是否有效運作？異常情形如何處理？在兩個角色的不同視角，很明顯資安經理人需要身心靈沉下去做事，稽核需要客觀來評估或判斷該作業設計及執行有效性。

應用新科技，站在巨人肩膀上飛行

以前準備 CISA 時，教材除了 Review Manual 及電腦稽核協會的認證研習班以外，若有不懂的地方，只能透過 Google 反覆查詢資料，知識零碎難以整合，經常為了某個觀念想不通，卡了好幾天。而現在我們有了生成式 AI，透過給予適當提示詞（Prompt），讓 AI 替我們釐清抽象或容易混淆的概念，若擔心 AI 輸出的內容幻覺太多，也能要求 AI 在輸出時附上資料來源，進而降低產生幻覺的機率。

但是當使用這項黑科技時，我認為身為人類的我們有幾件事必須謹記在心：

1. AI 可以用來釐清觀念、引導思路及整理資料，但「思考」這件事不能外包。
2. AI 用來解題很有用，但不見得是對的（幻覺永遠存在）。
3. AI 可以推著我們前行，不代表人類就能躺平，別浪費這位助攻巨人。

經常會聽到許多人說「用了 AI 做…我就可以非常輕鬆，什麼事都不用做…」，AI 確實可以幫我們做很多以前做不到的事，而這些事外包給 AI 後，我們人類能做些什麼？我們是站著等 AI 推著走，還是藉由 AI 助攻來跑得更快更遠？

或許 AI 已經重塑我們學習新事物的管道與方法，我們應該心懷感恩，同時謹守人類最珍貴的資產：腦袋，讓 AI 成為學習的助手，而不是讓它取代我們。

紀律與戰友的重要性

平日下班後拖著疲憊的身軀，只想躺在沙發上，假日更想遠離書堆與題目，但若真心想摘下這張認證，請「下定決心」。這個「決心」不是站在屋頂上向天空吶喊，也不是在情緒上頭時亂下的誓言，請意識到：你必須有紀律地安排時間、刷下那筆很貴的考試費，並且在多重誘惑下做出割捨。

我在備考過程中，要求自己不論上班有多累，回家洗完澡後題目至少要寫 20 至 30 題，並且將不懂或待釐清的問題或觀念，先請 AI 協助搜尋並彙整資料。隔天早上通勤途中，腦袋清楚的時候，將昨天 AI 彙整的資料拿出來讀，如有需要釐清或延伸的議題，再請 AI 彙整資料或引導思路，並且利用午休時間再讀一次，如此一來，從練習題→通勤途中複習→午休延伸複習，溫習三次後，觀念就不容易忘記，再搭配假日自行整理筆記或請 AI 代勞，就能持續累積需要強化或修正的知識與觀念。

另外，我也會將運動納入讀書計畫中，為什麼？上班工作，下班念書都要燒腦，適當的運動能幫腦袋好好洗個澡，將紊亂思緒梳理成條理分明的路線圖，讀書之餘去運動一下，讓知識流動更順暢、吸收更扎實。

而備考期間，很幸運在協會認證班認識的同學小強，他是資安領域的前輩，我們都有拿下 CISM 的決心，同時也在忙碌工作中準備考試，深知這段路程之不易，在準備過程中相互砥礪、交流、分享經驗，最終也跟上他的腳步取得 CISM。我想說的是，我很幸運有願意為共同目標努力的戰友，若您在準備考試的過程也有這樣的角色，請好好珍惜。

結語

準備 CISM 的過程，像是一趟視角校正與擴展的修行，理解稽核與資安管理兩種角色在同一風險議題上的不同語言與責任。從習慣以規範與證據客觀檢視作業循環，到學會站在資安經理人的位置規劃優先順序、設計補償性控制並推動落地。我很珍惜 AI 與戰友的助攻，而關鍵在於自己是否願意「下定決心」，騰出空間與時間，累積每天微小的進步，直到足以摘下屬於自己的底氣與機會，最後一句祝福送給大家：「只要目標在，路就不會消失」。