

從同理到實踐：設計思考 驅動資安審計培力

陳珮禎、方倉盛

（審計部第六廳薦任審計、薦任稽察兼科長）

資通安全管理法（下稱資安法）施行以來，公務機關資通安全（下稱資安）防護量能雖逐步提升，惟資安風險日新月異，多數審計人員亦非資通訊專業出身，資安查核職能落差成為審計機關落實資安監督之一大挑戰。審計機關運用「設計思考」方法，從問卷及訪談出發，規劃「訓用合一」資安培訓計畫，並研提專案調查，由中央與地方審計人員共組查核團隊，聯合辦理查核。

壹、前言

資安為數位治理的基石，做好資安才能建立可靠、隨時可用的政府服務。政府為積極推動資安防護，資安法自 108 年 1 月 1 日施行，導入資安弱點通報機制（Vulnerability Analysis and Notice System, VANS）、端點偵測及應變機制（Endpoint Detection and Response, EDR），公務機關資安防護量能雖逐步提升，惟資安風險日新月異，兼以地方政府資安人力、預算普

遍吃緊，資安防護仍面臨嚴峻挑戰。相對地，審計機關肩負監督政府資安治理成效之責，惟多數審計人員並非資通訊背景出身，對資安查核之風險識別、規劃及執行能力顯有不足，成為審計機關落實資安監督職能之一大瓶頸。

審計機關自 111 年度起舉辦政府審計創新共識營，審計部第六廳 112 年度透過籌組跨單位之創新團隊－數位及科技發展審計創新小組，設計「數位審計職能問卷調查」，發放 774 份問卷，回收 481 份有

效問卷，分初階審計人員、中階管理人員及高階管理人員三個層級進行分析。結果顯示，各層級審計人員普遍認為資安相關職能極為重要，但實際具備專業程度仍有不足。另針對 11 個中央及地方審計機關共 26 位人員進行深度訪談，進一步發掘職能落差背後的結構性原因，包括現行資安培訓課程與實務查核情境之連結尚待強化、資安領域專業門檻高但訓練時間過於短暫等，都讓審計人員即便有心投入，仍難以有效累積資安查核經驗。

面對此一困境，審計部第六廳運用「設計思考」方法，展開一系列以使用者需求為核心的探索與方案設計，逐步發展出「訓用合一」之資安培訓模式。

貳、現況分析

設計思考是一種以人為本的設計精神與方法（圖 1），旨在找出創新解決方案，滿足使用者的需求，不僅限於設計領域，

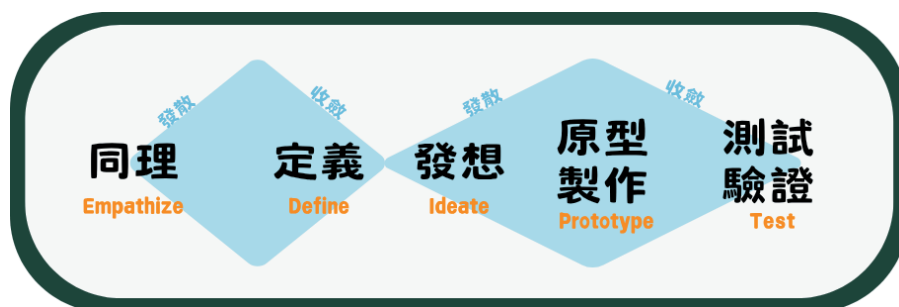
也廣泛應用於業務、科技、社會等各領域。

一、同理：從心出發，理解一線需求

第一階段「同理」的核心即在於放下既有假設，透過觀察、訪談與問卷等方式，真實理解使用者的處境與感受。審計部第六廳籌組跨單位之創新團隊，參考審計實務及專家學者意見設計問卷，蒐集審計同仁辦理數位審計之問題，針對資安之審計議題，深入訪談第一廳至第六廳、教育農林審計處，及新北市、宜蘭縣、花蓮縣、澎湖縣等審計處室共 26 位人員，訪談對象涵蓋初任審計（稽察）員至主管級人員，確保涵蓋不同職務層級的真實心聲。

受訪者表示，隨著被審核機關持續擴充資訊系統、增加資安預算，並將業務及資料管理逐步數位化，個人及機敏資料之蒐集與運用亦日益增加，使資安風險隨之上升，審計人員因而希望進一步充實相關知識。另於實務查核時，被審核機關可

圖 1 設計思考流程



資料來源：作者繪製。

能因資料涉及資訊系統、個人資料或機密內容，而對提供資料有所顧慮，審計人員在查核時間及人力有限之情況下，亦可能降低選擇資安議題之意願。另有受訪者指出，部分機關數位轉型程度較低，現階段較少感受到資安查核需求。就培訓經驗而言，現行課程多著重工具操作或講師經驗分享，與實際查核情境、議題選擇及查核切入方式之連結較少；加以課程多屬短期或一次性辦理，若未持續接觸相關知識，日後擬定查核議題時，可能不易回想或運用所學；資安領域涉及範圍廣泛且專業門檻較高，期待在實際查核過程中有專業人員陪同或提供指導，協助理解議題、掌握方向及累積經驗；由於查核期間通常橫跨數月，受訪者亦表達希望於查核過程中能有即時諮詢管道，以協助處理所遭遇的疑問與困難。

二、定義問題：聚焦核心癥結

設計思考的第二階段是「定義問題」。將問卷與訪談蒐集到的意見重新整理、分類與收斂，從中找出審計人員在查核資安議題時真正面臨的困難與需求。訪談顯示，雖然資安議題內容複雜、專業門檻也高，但多數審計人員其實都有意願接觸並查核相關議題。真正困難在於，現行培訓多以短期課程、工具操作或經驗分享為主，與實際查核情境的連結仍不夠緊密，

審計人員往往難以在有限時間內建立完整概念，也不容易把學到的知識轉化為可實際運用的查核方法。另一方面，在人力與時間都有限的情況下，審計人員若遇到資安專業問題，通常也缺乏可以即時請教的對象，從議題選擇、風險判斷到查核方法設計，都可能因此增加挫折感。綜合這些發現，本階段將問題聚焦在：審計人員缺乏完整的資安知識架構、貼近實務且持續性的培訓，以及可隨時提供協助的專業支持，因而不易有效規劃與執行資安查核，也影響進一步投入查核的意願。

參、創新查核技術方法

審計部為促進數位審計發展，於 111 年 1 月增設數位審計專責單位—第六廳，掌理數位及科技發展審計事項，並延攬具資訊及資安專業背景的人才，透過跨領域團隊的組成，強化數位與資安議題的查核量能。運用設計思考「發想—原型製作—測試驗證」階段，透過小組腦力激盪，提出業師陪伴、種子學員培訓、專業課程及案例分享等構想，並進一步收斂為「規劃訓用合一之資安培訓計畫」原型，由第六廳與地方審計處室查核團隊推動全生命週期之審計查核作業模式及培訓資安審計人才，聯合辦理「政府推動基層機關資安防護機制執行情形專案調查」加以驗證，茲將實踐過程說明如次：

一、查核規劃階段

由第六廳組成跨資訊科技、會計、工程等專業領域之數位審計查核團隊，於查核前召開 6 次專案調查規劃會議，擇選數位發展部資通安全署（下稱資安署）辦理之「強化政府基層機關資安防護計畫」、「政府基層機關資安主動防禦計畫」為專案調查範圍，並赴資安署辦理前導溝通會議，建立有效之溝通管道、掌握政策執行方針及相關調查表件內容妥適性，或洽其先行提供相關執行資料，逐步聚焦調查議題、分工方式及調查重點，並邀集地方審計處室同仁，以視訊方式召開資安培訓啓始會議，簡介資安相關法規與資通安全責任等級應辦事項、「政府推動基層機關資安防護機制執行情形」專案調查計畫等，以增進對資通訊科技查核領域之瞭解，並指派具資訊科技背景審計人員擔任地方審計機關資安專責輔導員。

二、就地查核階段

（一）組成聯合審計團隊：第六廳跨專業領域查核團隊，分三組聯合臺北市、新北市、桃園市、臺中市、臺南市、高雄市、基隆市、宜蘭縣、新竹縣、新竹市、苗栗縣、彰化縣、雲林縣、嘉義縣、嘉義市、南投縣等 16 個地方審計機關辦理就地查核，並擇選

新北市政府作為第 1 個示範查核場域，以利團隊後續分組至不同市縣政府查核時，能有一致性作業模式，並相互通報查核發現。

（二）訓用合一人才培訓模式：第六廳協同地方審計機關採順查方式針對資安防護機制管理流程（圖 2）進行查核，透過具資訊背景審計人員與被審核機關進行專業溝通，釐清技術細節，藉由「做中學」模式，強化審計人員對資安查核項目理解與掌握，暨透過審計作業模組化概念擬具資料蒐集清單，提供地方審計機關參考，有助傳承數位審計查核經驗及相互學習，提高審計工作效率及擴大整體審計成果，發掘整個政府系統性及結構性問題及其根源，並提出整體性建議意見，發揮審計綜效。

（三）分析跨政府資料以發掘資安風險，並開發數位審計模組：首次運用跨政府資訊資產檔案進行數據分析，蒐集 16 個市縣政府資訊資產清單，運用 Arbutus、Excel 及 Python 等工具，與國際權威弱點資料庫公告軟體弱點等資料進行比對，分析發現部分資訊資產（含中文軟體）未依主管機關指定格式轉換，影響後續資安弱點比對。另蒐集及整理非

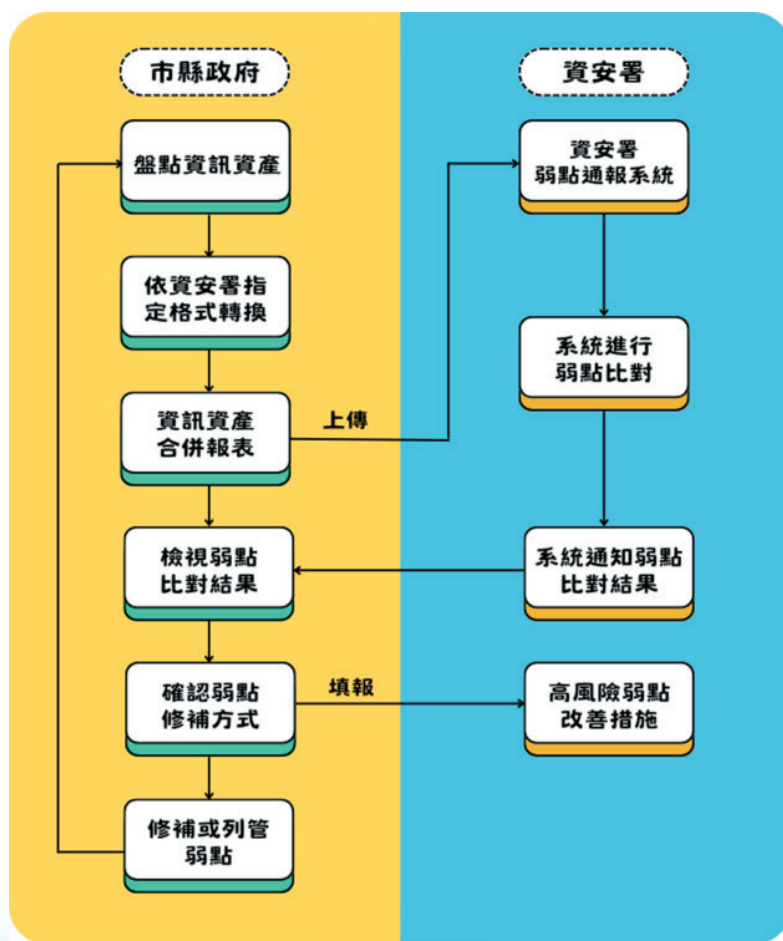
公務用軟體清單，搭配生成式 AI 輔助撰寫數位審計模組，將分析流程簡單簡化為 3 個步驟，使審計人員能快速取得分析結果，經比對發現，部分機關資訊資產存有資安風險軟體（如 Zoom），或安裝非公務使用軟體等情事，公務電腦恐有安全漏洞之虞。

三、報告撰擬及結果處理階段

為傳承數位審計查核經驗、縮短作業

時間及提升審計成果，納入數位審計模組概念，針對共同性缺失由第六廳統一撰擬查核意見範本，供地方審計機關善加運用後續發審核通知，達知識擴散之成效，並有助中央審計機關至地方審計機關查核意見連貫，及地方審計機關間之查核意見一致，見樹亦見林。於結果處理階段，由各主責地方審計機關繕發審核通知予被審核機關檢討妥處，後續可洽第六廳協助檢視行政機關覆核意見及提供建議核復意見。

圖 2 資通安全弱點通報機制管理流程



資料來源：作者依資安署提供資料繪製。

肆、審計成果與影響

一、擴展審計機關資通訊科技查核領域，提升資通訊科技查核技術軟實力

訓用合一模式推動後，已培訓數十位非資訊背景審計人員具備資安查核實戰能力，並輔導其撰擬被審核機關查核意見逾 50 項，達成培訓與應用合一之目標，發揮人才培育、跨專業領域及跨審計單位交流與協同查核之綜效。

二、發揮聯合審計協力綜效，促請行政機關精進資安管理作為

經審計機關促請檢討改善，16 個市縣政府已陸續移除具資安疑慮或非公務用途軟體近千項，且資安署於 114 年 3 月 31 日通函各機關，要求相關產品於完成汰換前應採取適當配套措施。另核心資通系統導入資安弱點通報機制（VANS）及端點偵測與應變機制（EDR）覆蓋率分別提升至 83% 及 97%。數位發展部數位產業署並自 113 年 7 月起於資訊服務採購網揭露 VANS 及 EDR 測試合格或連通測試通過名單，供機關採購時參考，提升政府採購軟體品質。此外，資安署亦完成新版 VANS 系統開發，增設提醒及管理功能，並提供地方政府依實際需求調整資安防護作業的

彈性，使整體資安防護機制更貼近實務需要。

三、開發數位審計模組，擴大審計成果應用及擴散效益

本案善用市縣政府資訊資產資料，分析發現使用具資安疑慮或非公務用軟體，後續經運用生成式 AI 輔助撰寫數位模組及操作說明，可供政風室、資訊處內部資安管理檢查或其他審計機關外部查核應用，協助提升審計工作效能。

伍、結語

跨領域人才常被視為「T 型人才」，意指除擁有垂直縱深的專業（T 型垂直部分），同時也擁有跨領域知識的橫向理解（T 型橫向部分），能夠在不同領域間進行有效協作及溝通。現今政府審計工作涉及範圍及複雜性日益擴大，其中數位審計為審計機關當前業務發展重點之一，T 型人才對審計機關的重要性也愈加突出，審計人員除善用聯合審計機制，透過跨審計機關、跨專業領域協同合作外，亦需順應政府數位轉型，自我發展數位審計斜槓思維及能力，除基本財務會計或公共政策分析專業知識外，應持續擴展並累積不同查核領域，舉如人工智慧、大數據分析、資通安全、資通訊科技等，以滿足多面向且複雜之審計需求。❖