我國數位鑑識國家標準規範之建議

陳受湛[1] 鄭健行[2] 吳佳翰[3] 宋子莉[4]
法務部調查局資通安全處 勤業眾信聯合會計師事務所
[1]dan-chen@seed.net.tw [2]safenet@mjib.gov.tw [3]chiahwu@deloitte.com.tw
[4]lsung@deloitte.com.tw

摘要

本研究係針對數位鑑識實驗室規範適用之管理與技術能力、數位鑑識人員與工具等方面進行審核與認證機制進行探討。過程中參考美國、英國、中國大陸等已有國際認證數位鑑識機構國家，進行各項審核與認證機制的演進作法與趨勢研究。最終將各國作法進行分析歸納比較，提出適於我國國情之審核與認證機制方式，並規劃出數位鑑識實驗室、人員與工具的具體做法與推動期程建議。

關鍵詞：數位鑑識、數位鑑識實驗室、數位鑑識認證機制

壹、前言

數位鑑識最早起源於國際電腦調查專家協會(IACIS) 提出之研究，在歐美等海洋法系國家因司法訴訟攻防取證等強烈需要，而使數位鑑識領域得以蓬勃發展且受到重視。因採用數位鑑識技術產出的數位證據必須用於法庭中輔助判決，若執行人員所表現知識或能力不足以勝任數位鑑識技術要求，勢必造成訴訟辯方反駁而法官可能會不採信專家證人的證詞[1]。英國下議會科技委員會[2]的研究報告也指出，用於產出證據的科學技術或理論都必須建立有效性證明，該證據方能被用於法庭訴訟。而 Guo, Slay & Beckett[3]的研究中也同樣指出，數位證物的蒐集、保存與分析都依賴著數位鑑識軟硬體，若工具或執行步驟有誤，都將使產出的成果證物在法庭上失去證據能力。

Slay 等幾位學者[4]在研究中提到，數位鑑識成果之品質強化來自於幾點要素：經國家認證實驗室、經資格認證專業人員、有效步驟與工具的運用。在美國監察長廉正及效率聯席會議[5]所發佈的規範中指出，數位鑑識確保品質的最低標準可區分為二：管理面標準，乃是關於數位鑑識執行的組織與環境，及其建立的政策與作業依循步驟，以做到鑑識能力與品質之管理；人員面標準，則是數位鑑識執行人員，可分為檢查分析人員與證據保全人員，對其資格與能力之基礎要求。

在 Sommer[6]的研究中指出，有集中化的資源才可更容易地公正評估鑑識人員的能力價值，而為司法體系所接受。在 Sabeil 等人[7]的研究認為透過資格認證與作業品質之評估，可有助於數位鑑識調查人員的職能強化。在 Guo & Slay[8]的研究中表示，任何數位鑑識工具的有效性與驗證，都應在正式使用前完成，才能確保信賴度與可靠性。Yang &

Yu[9]則認為產出司法可接受且精確的數位鑑識報告是數位鑑識實驗室建立目的之一，因此整體環境規劃、人員資格、專業領域、軟硬體要求與實驗室認證都需納入考量。

目前我國對於數位鑑識領域並無制定國家級標準規範，在國內有志參與數位鑑識實驗室、人員與工具發展等相關單位，都僅能各自仿效國外作法或自行摸索實驗，數位鑑識整體發展無益且緩慢。有鑑於此，本研究將以國家級標準規範為研究主軸，結合因應個人資料保護法之實務作業程序。以國際要求規格研擬數位鑑識實驗室、人員與工具之資格能力要求，以及審核與認證規範，以期做為政府機關與民間單位的實務參考。

貳、 文獻探討

一、標準之探討

「標準」一詞根據 ISO/IEC 2:2004 Guide 之定義[10]摘譯為：因共識而建立，且由公認機構核可，提供為普遍與重覆使用，予各種活動及其結果做為規則、指引或特性之文件，意欲達成既定情況下的秩序最佳化。而在我國標準法第三條第一款明定：標準是經由共識程序，並經公認機關（構）審定，提供一般且重覆使用之產品、過程或服務有關的規則、指導綱要或特性之文件。

全球推行各種標準化已歷史悠久，在標準之實際適用上，可區分為公司、團體、國家、區域與國際等五種體系層次[11]，如圖 1，標準的類型可分類為基本標準、術語標準、測試標準、產品標準、流程標準、服務標準、介面標準、提供資料標準等八類[10]，也可再依產業特性區分為不同領域。如定義中所提及，各類型標準亦可能有交互參照關係，依據各領域之發展施行程度，常見為兩種類型，如良好的國際標準經參照翻譯後變為國家內之施行標準；抑或是某特殊領域國家標準發佈後，受到國際組織之參考修訂後，發佈為新版國際標準。

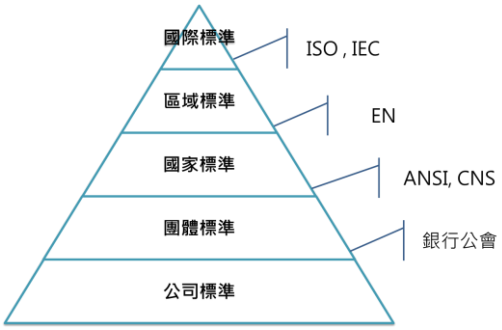

圖 1 標準體系關係圖

二、標準化制度

「標準化」一詞根據 ISO/IEC 2:2004 Guide 之定義[10]摘譯為：為考量實際或潛在問題，而制定普遍與重覆使用的規定之活動，意欲達成既定情況下的秩序最佳化。而標準化之效益對於產業發展的通常幫助為，需有一套標準作法，使參與者有均一的約束力與遵循方向，才不至於走向各自為政與主觀行事的發展局面；因此唯有標準化規範的建立，才能使工作進行或系統運作有規則可依循，管理評估方面才有較為客觀之依據。我國的標準化發展，係由經濟部標準檢驗局為主責單位，並依據「國家標準制定辦法」制定與實施，然而依據我國標準法第四條所述：國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。由此可知，國家標準雖然由國內各組織單位自願性遵循，但若納入為法規內文明令時，將成為強制性規範。

綜理以上論述，與訴訟有密切相關的數位鑑識領域實屬與民生安全相關之技術，我國現行數位鑑識產業發展則仍處於不同學術與商業公司之各自表述狀態，確實有數位鑑識國家標準規範建立必要。本研究擬將各國數位鑑識相關標準規範進行歸納分析，並提出適用於我國現況之建議內容。

參、數位鑑識國際間標準規範制度探討

一、數位鑑識實驗室管理能力審核與認證現況

（一）英國

英國乃為致力於發展標準化體系之國家，在標準認證制度與數位鑑識發展上都具備相當規模，更有專門的國家級標準制定機構-英國標準協會(British Standard Institution)專門推行各類國家標準，與 ISO 體系也有眾多相互合作接軌之處。隸屬於國內事務部之鑑識科學監管局(Forensic Science Regulator)，於 2012 年發佈專屬於數位鑑識領域的補充要求《實務與行為守則之附錄：數位鑑識服務》[12]之諮詢草案版本（擬定於 2013 年將意見回饋做後續修訂），明確地要求所有現行具備數位鑑識實驗室功能之服務提供者，並需於 2015 年 10 月之前通過 ISO/IEC 17025 認證；而文件中除了增加說明適用數位鑑識領域的遵循守則，並且更進一步要求進行數位鑑識現場調查服務提供者，應通過屬於檢驗(Inspection)機構領域之 ISO/IEC 17020 認證。

（二）美國

美國是世界上具備最多鑑識實驗室之國家，根據官方網站登載之已認證實驗室數量統計，屬於專業數位鑑識實驗室則為 20 所。然而因美國政治體制的特殊性，除了自願性

認證單位外，迄今僅有四個州政府對於州內所有鑑識實驗室具有強制認證要求[13]。而在審核認證要求方面，於 2006 年 ASCLD/LAB 組織制定出《ASCLD/LAB 國際測試實驗室: 補充條款》[14]以做為鑑識實驗室之補充要求。而 2011 年之《數位證物實驗室品質手冊》[15]由 FBI 合作數位鑑識社群 SWGDE 所發佈，亦為美國數位鑑識實驗室尋求認證時之研究參考。

（三）中國大陸

中國大陸之鑑識實驗室發展與國家層級有密切相關，除國際認證 ISO 體系外，並已自行發展出完整國家型認證標準。中國大陸實驗室審核機制說明可參照下圖 2，首先任何鑑識實驗室必須先申請且獲得效期五年之「司法鑑定許可證」，該機構才能合法設立與執業[16]，而在申請時必須滿足相關條件，如資金、設備、環境與人員等基本要求(可參照表 1)，且必須參加司法鑑定執業責任保險或建立執業風險金制度。

在正式執業運行後，實驗室可選擇取得接軌國家標準的「資質認定」（又因適用規模不同可分為省級與國家級），或是接軌國際標準的認證（於中國大陸使用詞彙：認可），藉此對實驗室自身的條件資格與能力進行評估，並對公眾證明其品質符合國家或國際標準。

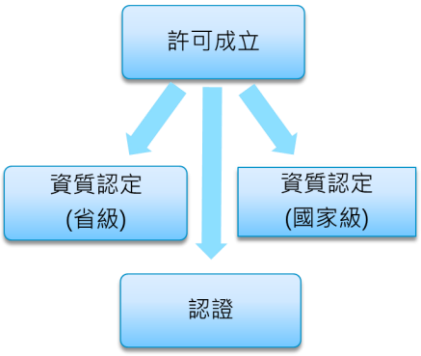

圖 2 中國大陸實驗室審核機制

表 1 民間機構執業之「司法鑑定許可證」申請條件

申請條件	內容
基本	固定名稱、住所
資金	不少於 20 萬~100 萬人民幣資金
業務	明確司法鑑定業務範圍
設備	必須之儀器、設備
環境	有司法鑑定必須之測試實驗室
人員	每項業務司法鑑定業務有三名以上鑑定人

中國大陸對於鑑識實驗室之態度，是以政府力量逐步推動全面性認證。在 2012 年最新頒佈的《關於全面推進司法鑒定機構認證認可工作的通知》，該法令對於認證要求已放寬為，新設立機構在核准登記後 2 年內通過資質認定或認證(中國大陸詞彙：認可)，已成立者在緩衝期限內完成即可。

（四）綜合觀點比較

綜觀以上各國數位鑑識實驗室審核/認證發展現況，歸納與分析出下表 2 之幾個比較面向探討，包含推動發展方式、認證申請是否有基本要求、是否有一致性審核/認證適用標準規範以及其他各國特色說明等。

表 2 各國數位鑑識實驗室認證特點比較

規範比較	英國	美國	中國大陸
推動發展	認證強制性	僅部分區域/ 領域強制	認證強制性
審核申請 基本要求	無	無	有條件限制
認證核心 要求規範	ISO/IEC 17025	ISO/IEC 17025	ISO/IEC 17025
數位鑑識領域 要求規範	官方發佈	數位鑑識社群 發佈參考手冊	官方發佈
各國特色	進行現場調查者另需通過 ISO/IEC 17020 認證	➢ 各州自主決定 ➢ 聯邦單位多自行主動通過	➢ 國家登記管制 ➢ 機構責任保險制度 ➢ 認證申請條件限制 ➢ 設國家標準區分中央與地方適用規模

二、數位鑑識實驗室技術能力審核與認證現況

（一）美國

因數位鑑識領域實驗室之新興性與特殊性，美國各界並無發佈適用於數位鑑識領域的標準檢驗方法，故現行（2013）公正機構所舉辦之能力試驗並無數位鑑識領域之指定項目。因此目前針對數位鑑識實驗室技術能力審核方式，如美國國家標準技術研究所之國家自願實驗室認證計畫 NVLAP[17]，皆為遵循 ISO/IEC 17025 規範原則。在實驗室審核認證期間，以實驗室內自行開發後明定為規範程序之一部，且經實驗室自行確認過之

檢驗方法，由實驗室人員執行實作，並由認證組織之評鑑人員確認成果以評定該實驗室的技術能力水準。

（二）中國大陸

中國大陸已於 2008 年由公安部發佈適用於數位鑑識領域的標準檢驗方法(證據保存類)，雖然於規範被定義屬於推薦性之非強制行業標準，如表 3 所示，但已被陸續採用作為實驗室申請認證時的技術項目，並成為 2011~2013 每年中國大陸官方舉辦之數位鑑識領域能力試驗計畫之指定試驗項目。於 2012 年，中國合格評定國家認可委員會再發佈推薦性之國家標準，其中也包含資料復原與關鍵字搜尋之相關技術規範，可預期在未來將成為申請認證的技術項目與標準檢驗方法之官方依據。

表 3 中國大陸數位鑑識技術方法相關標準規範

標準編號	名稱
GB/T 29360-2012	電子物證資料復原檢驗規程
GB/T 29362-2012	電子物證資料搜索檢驗規程
GA/T 756-2008	數位化設備證據資料發現提取固定方法

二、數位鑑識人員資格、規範、審核與認證現況

（一）英國

英國是最早開始鼓勵鑑識人員自願性審核登記之國家，然而 2009 年時鑑識科學監管局從原 CRFP 協會審核之方式，轉由英國認證服務組織(UKAS)所取代，而成為英國國內唯一專責認證機構[18]。英國政府態度開始趨向以實驗室整體品質要求取代個人能力評定，人員能力被視為附屬為鑑識實驗室認證範圍內之一環，不再獨立登記[19]。而 2010 年起，因英國訴訟制度仍存有聘請鑑識專業人員之需求，民間鑑識科學學會(FSSoc)因此開始自行推廣該協會的鑑識從業人員審核登記，前述三種單位人員要求，如表 4 所示：

表 4 英國數位鑑識人員要求比較

人員要求	CRFP 協會審核	實驗室認證	FSSoc 學會審核
背景檢查	無	個人背景檢查	單位主管背書證明
執業承諾	承諾品德聲明	承諾保密與遵守資安聲明	承諾品德聲明
專業能力	合格專業資歷	依據 ISO/IEC 17025 規定(人員職能相符)	合格專業資歷證明
推薦人	專業推薦人	無	證詞技能推薦人

工作評估	合格之近期案件匿名性工作成果	無	合格之一年內案件工作成果
問題考核	專業評鑑員進行評估及指定問題回覆	無	無
工作經驗	無	無	三年以上工作經驗
持續發展	無	無	三年以上持續專業發展證明

（二）美國

美國是具備多種數位鑑識人員培育管道之國家，除學士與碩士專業課程外，亦提供最多種數位鑑識人員類國際證照。但如前文所提及，美國各州自治之自由開放態度也導致對於數位鑑識人員之資格或審核要求並無任何一致性規定。僅有部分單位，如美國監察長廉政及效率委員會(CIGIE)與 SWGDE，提出較明確建議人員資格要求[20]，如表 5 所示：

表 5 美國數位鑑識人員要求比較

人員要求	CIGIE 建議	SWGDE 建議
專業能力	• 電腦運作、資料傳輸與儲存之技術知識 • 不同類型電腦設備障礙排除能力	負責報告解釋人員應有足夠訓練、經驗與檢驗知識
證照要求	參與數位鑑識訓練測驗課程，或取得正式證照	技術人員於特殊領域需有證照要求
工作經驗	適當工作經驗（或以較長工作經驗取代大學學歷）	無
教育要求	四年制大學學歷，含電腦與網路運作完整技術原理	技術人員應符合職掌之教育背景，至少為理學士

（三）中國大陸

中國大陸對於數位鑑識人員之管控，亦採取中央統一管理之作法，在 2006 年公布之《司法鑒定人登記管理辦法》法令，明定出需由預計執業的鑑定機構替人員提出申請，審核登記後取得效期五年之「司法鑑定人執業證」始可執行業務[21]，而採用將鑑定人與鑑定機構導向一同綁定管理之作法。

並透過司法鑑定管理局之監督，省級司法行政機關之行政管理，以及各省司法鑑定行業協會之行業管理，將司法鑑定人的執業資格進行控管，並由所屬行政管理單位建立「司法鑑定人誠信檔案」對外公開發佈，以受社會大眾之公評與檢視。

而在對數位鑑識人員的資格審核要求方面，依據官方管理辦法，以及前述之機資質認定與認證，各有不同層面的明確要求，於表 6 中做一歸納比較。

表 6 中國大陸數位鑑識人員要求比較

人員要求	司法鑑定人登記管理辦法	檢測和校準實驗室能力認可準則在電子物證檢驗領域的應用說明	司法鑒定機構資質認定評審準則
執業承諾	遵守法律、法規與公德之公民	無	無
專業能力	無	無	相應的資格、培訓、經驗，熟知所從事鑒定的規則和要求，並有做出專業判斷和出具司法鑒定文書的能力。
工作經驗	具備相關專業工作十年以上經歷與較強專業技能	應在本專業工作 5 年以上，或具有本專業高級技術職稱。	具有司法鑒定人資格並同時具有副高級以上本專業領域的技術職稱，或者取得司法鑒定人資格後在本專業領域從業 5 年以上。
教育要求	相關高級專業技術職稱;或相關行業執業資格或高等院校相關科系大學以上學歷,從事相關工作五年以上	應具有電腦科學專業、電子技術專業或者相關專業大學本科以上（包括大學本科）學歷，或者具有同等學歷，且經過電子物證檢驗技術方面的技術培訓，並至少具備在電子物證檢驗領域的 3 年工作經驗。	無
體格要求	身體健康可適應司法鑑定工作需要	無	無

（四）綜合觀點比較

綜觀以上各國數位鑑識人員資格規範與審核認證發展現況，歸納與分析出下表 7 之

幾個比較面向探討，包含推動發展方式、是否有一致性審核/認證適用標準規範以及人員資格發展方式等。

表 7 各國數位鑑識人員要求特點比較

規範比較	英國	美國	中國大陸
推動發展	➢ 以實驗室認證代替人員審核登記 ➢ 民間學會推動登記	無審核登記機制	審核通過才可執業
審核認證官方要求	有	僅組織內部建議	有
實驗室認證之人員要求	➢ 依 ISO/IEC 17025 ➢ 另有補充規範要求	➢ 依 ISO/IEC 17025 ➢ 另補充規範要求	➢ 依 ISO/IEC 17025 ➢ 另有補充規範要求
人員資格發展方式	具備專業學術教育	較多國際證照培育 較多專業學術教育	較少專業學術教育

三、數位鑑識工具審核與認證現況

（一）美國

目前美國官方針對工具標準化之工作委由國家標準技術研究所(National Institute of Standards and Technology，以下簡稱 NIST)所屬的電腦鑑識工具測試計畫(Computer Forensics Tool Testing Program，以下簡稱 CFTT)負責研究與開發。測試標準分類係依工具功能而劃分，但由於此領域之新穎與技術變動速度快速，故目前官方正式完成的標準僅有磁碟映像檔製作之測試方法論，以及軟體防寫工具測試方法論之標準最終版本發佈；刪除檔案回復則是預計即將進行之測試計畫。另外，其他數位鑑識領域功能，例如字串搜尋、硬體防寫工具、手機鑑識工具等也已有相關草案[22][23]。

數位鑑識工具審核機制主要由 CFTT 之主導委員會(Steering Committee)決定應測試之工具為何，雖然業者亦可主動提出要求對其產品進行測試，惟最後決定仍由主導委員會裁定，並不同一般產品驗證概念之申請即可進行測試。而後完成測試之工具由 NIST 組織製作測試報告，再交由主導委員會與工具廠商審核。最後由 NIST 與國家司法協會(以下簡稱 NIJ)將測試報告發佈於網站予公眾參閱。

（二）中國大陸

中國大陸現行的標準制度依適用範圍分為：國家標準、行業標準、地方標準、企業標準。國家標準與行業標準又各自分為強制性與推薦性兩類。目前在中國大陸之工具測試標準皆屬於推薦性，如表 8 所示，即由各企業自願性採用，而目前並未有相關產品申請並通過此類標準。中國大陸於數位鑑識領域的標準發展時間不長，而然已發佈之工具功能相關規範數量較多，但其中針對映像檔製作工具與防寫工具亦有明文發佈國家級檢測方法，惟其檢測方法內容之詳細度遠不如美國 CFTT 計畫中所制定檢測方式。

表 8 中國大陸數位鑑識工具功能相關規範

標準編號	名稱
GA/T 754-2008	電子資料儲存媒體複製工具要求及檢測方法
GA/T 755-2008	電子資料儲存媒體防寫設備檢測方法

根據中國大陸公佈之標準化法[24]第 15 條規定：企業可以向國務院標準化行政主管部門申請產品品質驗證（中國大陸詞彙：認證）。目前其標準化行政主管部門為國家品質監督檢驗檢疫總局(以下簡稱質檢總局)。另又分將標準化與認證認可之任務分派予國家認證認可監督管理委員會(以下簡稱認監委)與國家標準化管理委員會(以下簡稱標準委)。故驗證（中國大陸詞彙：認證）事務掌理為認監委。又認監委根據中國大陸公佈之認證認可條例設立合格評定國家認可委員會(以下簡稱認可委)，統一負責對驗證機構、實驗室和檢驗機構等相關機構的認證工作，因此由希望進行產品驗證之廠商向驗證機構申請認證之服務。

（三）綜合觀點比較

綜觀以上各國數位鑑識工具審核與認證發展現況，歸納與分析出下表 9 之幾個比較面向探討，包含審核工具選擇、工具檢測方法論、方法開發與結果呈現等。

表 9 各國數位鑑識工具審核特點比較

特點比較	美國	中國大陸
審核工具選擇	CFTT 委員會自行決定 可接受工具廠商推薦備選	工具廠商可向驗證機構申請產品驗證
已完成工具檢測方法論	磁碟映像檔製作功能 軟體式防寫功能	➢ 儲存媒體複製工具 ➢ 儲存媒體防寫設備
方法開發	NIST 之 CFTT 委員會主導	➢ 國務院標準化行政主管部門制定之國家標準 ➢ 公安部制定之行業標準
結果呈現	NIST 將測試報告公布於網站	驗證機構發放證書予工具廠商

肆、研究成果

一、數位鑑識實驗室管理能力審核與認證機制建議

基於數位鑑識產業之逐步興起，對於有意進入數位鑑識實驗室領域單位也陸續出現，經由分析各國數位鑑識實驗室審核與認證之發展近況後，綜理各國優點所提出較能符合我國國情之建議。

（一）審核制度及單位

為促使數位鑑識實驗室之運作，能以具有品質可靠度並與國際接軌方式獲得認可，建議採用現行國際標準實驗室認證體系做為審核制度，應為符合世界潮流趨勢之最佳做法，且應結合政府力量推動民間發展，擇定數位鑑識實驗室產業的主導單位，以監督標準化進行。茲建議如下：

1. 審核/認證單位：TAF 全國認證基金會

   因全國認證基金會為我國唯一主管合格性評鑑機構，實驗室認證(Accreditation)為其運作業務之一，因此數位鑑識實驗室依循著國際 ISO/IEC 17025 標準應以 TAF 組織為唯一評鑑單位。
2. 主導單位：行政院轄下單位（如法務部、標檢局等）

   因數位鑑識為實驗室的特殊新興領域，具備法律與科學等跨範疇特點，應協助制定且確認數位鑑識實驗室適用之標準方法，使政府機關與民間實驗室之業務執行得以有公正依據。

（二）認證機制

與各國發展現況相比，我國目前缺乏數位鑑識領域適用之實驗室認證補充規範，以致於有心從事實驗室認證之單位仍保持觀望或仍在自行摸索狀態。有鑑於此，欲完備我國數位鑑識實驗室認證標準規範，茲建議發展方向如下：

1. 制定 ISO/IEC 17025 適用之數位鑑識領域認證技術規範

   應以 ISO/IEC 17025 要求為基底，延續規範要求的管理面與技術面規定，將適用於數位鑑識領域之條款增訂補充性條款，以協助數位鑑識實驗室參與者能有明確依循，進而使產業發展更易成長。此項規範之制定，建議可透過 TAF 全國認證基金會與數位鑑識領域相關學會於共同合作基礎下共同完成，以便同時符合 ISO 規範之原則，亦達成技術水準之要求。

（三）數位鑑識領域標準試驗方法制定與能力試驗舉辦

ISO/IEC 17025 重點要求為，必須有能力試驗的參與紀錄以藉此檢測與證明數位鑑識實驗室技術能力，而能力試驗之依據為共識性試驗方法；但因數位鑑識領域的特殊性，並未有國際間明確有共識之標準試驗方法產生， 故亦建議應有政府級單位主持制定適用項目之通用性試驗方法以作為能力試驗的檢測標準。

（四）數位鑑識實驗室技術能力審核實務建議

由前述探討的能力審核方法可知，實驗室之技術能力審核與認證確為實驗室整體認證制度之一環。且唯有標準試驗方法之制定與發佈，對於技術項目之能力實作審核，或技術能力之公開性審核（即實驗室認證機制下之能力試驗），抑或是協議邀約之同儕性審核（即實驗室認證機制下之實驗室間比對），才具有較佳之一致性審核基礎。而數位鑑識技術能力之試驗方法有其特殊性，依據 ISO/IEC 能力試驗導引[25]與要求[26]之原則判定，數位鑑識技術能力之測試方法皆屬於定性分析，不同於一般定量分析方法之量測需要，故並無計算統計數據之必要。再者，定性類分析之技術能力審核方法亦以審核專家之共識意見為其典型評估方法。

因此綜觀美國鑑識科學實驗室主管學會/實驗室認證委員會之能力試驗與審視計畫[27]、國際實驗室認證組織之能力試驗導引[28][29]中對於能力試驗要求之原則與精神，以及參考中國大陸數位鑑識技術方法之行業標準[30][31][32]所陳述之實務作法，提出通用性審核機制說明，並分別就三種常見數位鑑識技術項目之試驗方法，提出技術面實務審核建議。惟此技術能力審核機制有其前提，無論採用公開性審核或邀約性同儕審核，需有審核單位或邀約單位依據 ISO 規範與 ILAC 發佈對能力試驗指引[29]，所妥善製作與管理之試驗件，以便於證明後續試驗之公正性。

（五）通用性技術能力審核機制

參照 ISO/IEC 17043[25]所敘述之定性類技術能力審核方式，此方法需由符合 ISO 體系標準且能合格舉辦能力試驗之公正審核單位，預先準備好具一定特性(設定值)之試驗件，提供參與實驗室進行分析。再由參與實驗室將分析結果回傳與設定值比對是否為相同結果即可。因此考量數位鑑識領域之特性，茲建議技術審核機制如下：

1. 對審核單位提供之試驗件進行記錄（包含各種參數與外觀照片）。
2. 準備試驗所需設備（包含硬體設備與儲存媒體之設置）。
3. 執行與記錄試驗技術項目（包含攝影與書面）。
4. 進行試驗結果封存（包含雜湊值與檔案等）。

5. 進行結果紀錄封存（包含影音檔或儲存媒體）。
6. 試驗結果提供予審核單位（包含書面報告與影音檔等）。

（六）證據保存技術項目

證據保存之技術原理為，在不變動原始儲存媒體之情況下，利用鑑識工具將儲存媒體進行完整位元複製，且兩者內容經過計算驗證為完全一致，而將複製後的媒體或檔案做為後續的實務分析目標，以保存原有的儲存媒體內容做為原始證物。茲建議技術審核方式如下：

1. 將審核單位提供做為試驗件之儲存媒體 A 進行雜湊值計算。
2. 對儲存媒體 A 製作鑑識性映像檔，且計算該映像檔的雜湊值，且該鑑識性映像檔之雜湊值應與儲存媒體 A 本身之雜湊值相等。
3. 此雜湊值與該鑑識性映像檔即為應提供予審核單位之結果。

（七）資料復原技術項目

資料復原之技術原理為，在不變動原始儲存媒體之情況下，利用鑑識工具針對儲存媒體之內容進行復原，其復原標的為邏輯檔案被刪除後，仍存在儲存媒體磁區空間中，且為檔案所在磁區為尚未被覆寫狀態。

1. 將審核單位提供做為試驗件之儲存媒體 A 進行雜湊值計算。
2. 對儲存媒體 A 進行鏡像複製到儲存媒體 B。（儲存媒體 B 之容量應大於或等於儲存媒體 A，且複製後儲存媒體 B 之雜湊值應與儲存媒體 A 之雜湊值相等。）
3. 以防寫裝置對儲存媒體 B 進行指定之索引（如審核單位給定檔案名稱）進行資料復原操作。
4. 計算資料復原所得到之檔案之雜湊值。
5. 此雜湊值與該復原所得檔案即為應提供予審核單位之結果。

（八）資料搜尋技術項目

資料搜尋之技術原理為，在不變動原始儲存媒體之情況下，利用鑑識工具針對儲存媒體之內容進行指定關鍵字資料搜尋，其搜尋標的可能為邏輯性檔案或儲存媒體磁區空間（包含未配置空間、檔案殘餘空間等），以找出包含關鍵字之各種格式檔案或原始資料片段。茲建議技術審核方式如下：

1. 將審核單位提供做為試驗件之儲存媒體 A 進行雜湊值計算。

2. 對儲存媒體 A 進行硬碟複製得到儲存媒體 B。(儲存媒體 B 之容量應大於或等於儲存媒體 A，且複製後儲存媒體 B 之雜湊值應與儲存媒體 A 之雜湊值相等。)
3. 將儲存媒體 A 以封存程序進行封存。
4. 以防寫裝置對儲存媒體 B 以審核單位指定之索引（如審核單位給定檔案名稱）進行資料搜尋操作。
5. 計算資料搜尋所得到之檔案之雜湊值。
6. 此雜湊值與搜尋所得檔案即為應提供予審核單位之結果。

三、數位鑑識人員資格、規範、審核與認證機制建議

由前章文獻探討所述，可以得知各國對於數位鑑識人員之整體管理機制或資格認可方面做法皆有所不同，惟是否皆適用於我國環境則有待商榷，因此透過本研究報告所舉辦的訪談調查，以釐清各國考量要點於我國施行的適切性，故擇定現任實際從事數位鑑識分析實務工作之專業調查員進行意見瞭解，並將訪談結果整理分析。

（一）資格規範建議

在人員資格規範的探究方面，本研究參考各國機制而綜合歸納出六項考量要點做為意見探討項目，包含學歷科系、工作經驗、專業培訓等要求，以及背景檢查、推薦背書與實質工作成果檢查等機制，訪談調查之結果分析如下：

1. 學歷科系要求

   所有受訪者皆同意應至少為大學以上學歷，但過半數受訪者認為人員具備資訊電子相關科系背景較為優勢，因數位鑑識標的為資訊設備與相關原理，設定學歷科系背景要求對從事數位鑑識產業可有所助益。

2. 工作經驗要求

   所有受訪者皆同意且認為從事數位鑑識調查人員者，應具備資訊相關工作經驗至少二年，並有實務數位鑑識分析經驗至少二年（包含受監督之實習偵辦期間，且參與六案以上)；其原因為有相當工作經驗者，對於案件情境中所遇到各種實務環境都能快速上手處理。

3. 專業職能要求

   所有受訪者皆同意且認為在專業職能方面之最低要求為，至少曾參與數位鑑識訓練課程或科系學分且順利結業，並未要求必須取得國際鑑識專業證照。

4. 背景檢查機制

訪談結果發現，大多數受訪者並不傾向強制要求背景檢查，雖可要求從業人員出具警察刑事紀錄等相關證明，但對隱私保護可能有所爭議，且與工作無絕對直接相關。

5. 推薦背書機制

訪談結果發現，大多數受訪者並不傾向透過推薦背書機制認可數位鑑識人員資格，其因推薦人背書機制易流於形式，且難以有實質確定效果。

6. 實質工作成果檢查

從訪談中顯示，所有受訪者皆不傾向使用實質工作成果檢查機制，認同其對於承辦之工作案件內容可能違反保密協議。

綜合歸納以上鑑識分析人員觀點，發現實務界人士對於數位鑑識人員規範資格要求偏向技術能力之重視，這也符合本研究之宗旨所欲探求議題之一，即為數位鑑識人員應具備的資格能力。故提出數位鑑識從業人員規範資格建議如下表：

表 10　數位鑑識從業人員規範資格建議

規範項目	人員資格
學歷科系要求	大學以上學歷 資訊/電子相關科系為佳
工作經驗要求	資訊相關工作經驗至少二年 數位鑑識調查經驗至少二年（包含受監督之實習偵辦期間，且參與六案以上）
專業職能要求	曾參與專業數位鑑識訓練課程並結業

（二）審核及認證機制建議

人員審核與認證的探討方面，本研究參考各國機制而綜合歸納出三項考量要點做為意見探討項目，包含國家考試評斷、公正單位資歷查核登錄，以及依附國際標準實驗室認證等機制，訪談調查之結果分析如下：

1. 國家考試評斷

大多數受訪者認為，現階段國內環境並未成熟，產業市場尚未蓬勃發展，並不適合由國家舉辦考試機制。因數位鑑識人員目前並非為產業發達之職業市場，利用國家考試機制驗證資格恐不符合比例原則。

2. 公正單位資歷查核登錄

所有受訪者皆認為有專業且公正單位之成立（如數位鑑識學(協)會等機構），而作為人員資歷審核的主導機關，為最適合之人員登錄審核認可方式。透過與會學者專家針對申請者的數位鑑識產業資歷進行審核，並以公開合格人員專業資歷之方式可為社會大眾之公評與檢視。

3. 依附國際標準實驗室認證機制

在此一觀點受訪者意見較為分歧，半數受訪者認為並不應強制要求依附實驗室認證機制之原因為，許多個人亦有技術能力從事數位鑑識工作；但另一方意見則認為，結合實驗室國際認證機制，可確保人員與其執行環境與技術的整體適當性。結合 ISO/IEC 17025 國際認證之品質結果確認，可同時確保數位鑑識人員之分析結果品質，也可促使進入產業之組織單位必須具備全面性良好管理系統與環境設施，對民眾公平期待有更多保障。

綜合前述鑑識分析人員說法，普遍認為由公正單位進行人員資歷查核與登錄是最佳做法；但另一方面，由於結合了管理體系與實體環境之品質要求，隸屬於合格認證實驗室之人員也可視為審核管道之一；縱理以上觀點，本研究在兩者制度並行之預期下，歸納出對於人員審核認證機制建議如下表：

表 11　數位鑑識從業人員審核認證機制建議

類型	審核/認證機制
公正單位 資歷查核登錄	1. 由公正單位主導（如數位鑑識專業學會等） 2. 數位鑑識從業人員自願提出申請 3. 與會專家學者審核申請者之數位鑑識資歷 4. 合格者登錄於學會 5. 學會於公開管道發佈合格人員專業資歷
依附國際標準	隸屬於通過 ISO/IEC 17025 認證實驗室的數位鑑識分析人員，除持續符合實驗室自訂人員資格之教育、訓練、經驗與實作要求外，亦需在實驗室認證與定期審核時展現實驗室的技術能力。

四、數位鑑識工具審核與認證機制建議

由前述文獻探討可知，美國與中國大陸在數位鑑識領域之工具審核標準，雖然迄今僅限於少數類型功能/設備，但基於數位鑑識工具產出結果對訴訟攻防有其影響力，故兩國相關單位仍持續發展數位鑑識領域之工具檢測技術規範。若為國內引入未經國際檢測之鑑識產品或我國廠商自行開發之數位鑑識工具，可鼓勵參與工具檢測自願性認證，以

促進民間數位鑑識產業發展工具之可信度。

綜觀美國 NIST、中國大陸公安部之工具審核機制，以及參照現行我國推動之資訊安全設備檢測機制，茲提出適用於數位鑑識工具的建議如下：

（一）審核制度及單位

1. 審核單位：符合設備測試/評估資格之實驗室

   因數位鑑識工具審核屬於產品類型之測試，且基於其工具運用的特殊性，應為政府單位主導與認可，委由經過 TAF 全國基金會認證之公正第三方實驗室進行技術性測試/評估，憑藉測試報告之出具而使政府單位能對該項產品有審核依歸。

2. 主導單位：行政院轄下單位（如標檢局、NCC 等層級單位）

   因數位鑑識工具具備技術特殊性，應由主導單位協同專門技術學會訂定適用之檢測相關技術規範，其中包含功能需求與設計要求及其審查標準、測試案例與其判定標準，以便於民間產業在開發或檢核引入鑑識產品時，能有明確指引。

   1. 由主導單位與相關學會訂定與發佈檢測相關技術規範。
   2. 產品廠商依循相關技術規範進行自身產品規格確認。
   3. 產品廠商委請主導單位認可之審核單位執行產品檢測。
   4. 產品廠商向主導單位申請自願性產品驗證合格證明。
   5. 主導單位據取得資料進行產品驗證。
   6. 主導單位核發驗證證明予產品廠商，並公告做為公眾採購參考。

伍、結論與建議

一、結論

依據本研究報告之動機，針對數位鑑識實驗室相關之管理能力、技術能力、人員與工具等各方面進行研究，除了對數位鑑識領域發展熱絡的各國現況進行探討外，並以研討訪談進行方式吸收專業人士意見，建構出專屬於實驗室、人員與工具適用之審核與認證機制建議，以作為國家標準規範之參考依據。藉著本研究建構之內容，可提供政府推動一致性標準規範之基石，對於各界單位發展數位鑑識產業也具備正面意義之輔助。
本研究報告所達成之目的如下，預期成果可提供政府單位作為推動數位鑑識標準規範整體機制之規劃參考，以期提昇國內數位鑑識產業發展：

1. 在數位鑑識實驗室管理能力方面，綜理各國數位鑑識實驗室之發展演進與優點處，提出適於我國國情之鑑識實驗室管理能力審核與認證機制。

2. 在數位鑑識實驗室技術能力方面，綜理現行公信組織發佈之鑑識技術檢核方式，提出鑑識實驗室技術能力審核實務建議。
3. 在數位鑑識人員方面，綜理各國對於鑑識人員管理作法，以及對於人員多元資格要求等，結合實務人員訪談看法，提出鑑識人員資格、規範、審核與認證機制之建議。
4. 在數位鑑識工具方面，整合國際現有之美國與中國大陸觀點，並參照我國現行資安設備檢測作法，提出鑑識工具審核與認證機制建議。

二、建議

未來建議，我們短期、中期及長期目標來說明，如圖 3 所示：

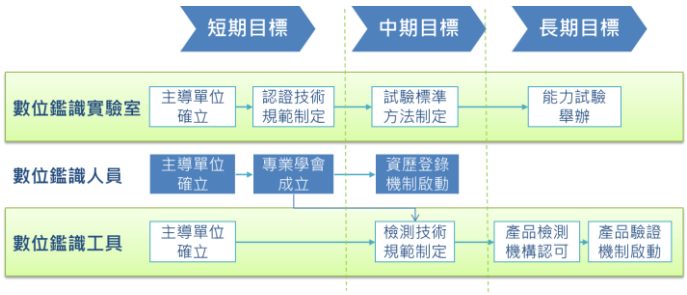

圖 3 未來建議

1. 短期目標

在短期內應確立各類審核與認證機制的主導單位，以便於整體認證機制的規劃與推動。在實驗室相關單位的主導單位成立後，可參照本研究之建議，商議擬定數位鑑識實驗室認證適用的技術規範。此外，透過專業學會的成立，可為後續的中期目標進行籌備。

2. 中期目標

在中期階段應可推動數位鑑識實驗室體系所需試驗標準方法之制定，使實驗室之鑑識分析方法更具標準化。藉由數位鑑識專業協會之運行，可啟動鑑識人員之資歷登錄機制，進而建立數位鑑識人才庫；並透過學會之技術專業能力，可研究草擬鑑識工具之檢測技術規範，為日後產品驗證奠定基底。

3. 長期目標

在本研究期望之最終目標，數位鑑識實驗室之主導機構可協助舉辦具備能力試驗，使所有實驗室領域參與者都能獲得具備公信力之評比機會。而在工具驗證方面，

經由國家認可數位鑑識產品檢測機構之成立，可最終達成產品驗證機制之建構。

參考文獻

[1] Fundamentals of Digital Forensic Evidence. Dr. Frederick B. Cohen, Ph.D. Fred Cohen & Associates and California Sciences Institute, 2008

[2] Science and Technology Committee, “Forensic Science on Trial”, 2005

[3] Yinghua Guo, Jill Slay, Jason Beckett, Validation and verification of computer forensic software tools-Searching Function, Digital Investigation: The International Journal of Digital Forensics & Incident Response, Volume 6, September, 2009, Pages S12-S22

[4] Jill Slay, Yi-Chi Lin, Benjamin Turnbull, Jason Beckett, Paul Lin, Towards a Formalization of Digital Forensics, IFIP WG11.9 Publications - Digital Forensics - IFIP11-9 , pp. 37-47, 2009

[5] Council of the Inspectors General on Integrity and Efficiency, “QUALITY STANDARDS FOR DIGITAL FORENSICS”

[6] Sommer P. Certification, registration and assessment of digital forensic experts: The UK experience. Digital Investigation 8:8 (2011)

[7] Sabeil, E., Manaf, A.B.A., Ismail, Z. and Sarkan, H.M., “Development of Malaysian's Digital Forensics Investigation training/education programs Quality Assurance and Accreditation”, E-Learning and e-Technologies in Education (ICEEE), 2012, pp. 204-208.

[8] Yinghua Guo, Jill Slay: Data Recovery Function Testing for Digital Forensic Tools. IFIP Int. Conf. Digital Forensics 2010: 297-311

[9] Chung-Huang Yang & Shan-Liang Yu, Sec-03. The Establishment of Digital Forensic Laboratory. 2011 第七屆知識社群國際研討會

[10] International Standard Orgnazation, ”SO/IEC GUIDE 2:2004”, 2004

[11] 洪安寧，”從產業專利爭議論產業標準化相關法律問題”，2004 年。

[12] Forensic Science Regulator, “Codes of Practice and Conduct Appendix: Digital Forensic Services”, FSR-C-107-001, 2012.

[13] Mozayani, A., Noziglia,C.,The Forensic Laboratory Handbook: Procedures and Practice,Humana Press, 2005

[14] ASCLD/LAB , ASCLD/LAB-International - Program Applications, Guidance & Board Interpretations, 2011,

[15] Scientific Working Groups on Digital Evidence and Imaging Technology, “SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence”, Version 2.0, Jan 2010

[16] 中華人民共和國司法部令，司法鑑定機構登記管理辦法，2005 年。
[17] C. D. Faison, J. Horlick, W. R. Merkel, V. R. White, National Voluntary Laboratory - Accreditation Program Procedures and General Requirements, 2006
[18] Home Department, Council for the Registration of Forensic Practitioners , 2009
[19] Forensic Resources Limited , Forensic Science Accreditation , 2009
[20] Council of the INSPECTORS GENERAL on INTEGRITY and EFFICIENCY, QUALITY STANDARDS FOR DIGITAL FORENSICS, 2012.
[21] 中華人民共和國司法部令，司法鑑定人管理辦法，2006 年。
[22] “Forensic String Searching Tool Requirements Specification”, Public Draft 1 of Version 1.0, January 24, 2008
[23] "Active File Identification & Deleted File Recovery Tool Specification", Draft for comment 1 of Version 1.1
[24] 第七屆全國人民代表大會常務委員會第五次會議, “中華人民共和國標準化法”, 1988
[25] International Organization for Standardization, ISO/IEC 17043:2010 Conformity assessment -- General requirements for proficiency testing, 2010
[26] 財團法人全國認證基金會, ISO/IEC 17043:2010 符合性評鑑－能力試驗的一般要求能力”, 能力試驗執行機構認證規範 TAF-PTP-R01(1), 2011
[27] ASCLD/LAB, ASCLD/LAB Proficiency Testing and Review Program, 2011
[28] International Laboratory Accreditation Cooperation,“ILAC G22:2004 Use of Proficiency Testing as a Tool for Accreditation in Testing”, 2004
[29] International Laboratory Accreditation Cooperation,“ILAC-G13:07/2007 ILAC Guidelines for the Requirements for the Competence of Providers of Proficiency Testing Schemes”, 2007
[30] 中華人民共和國公安部, 中華人民共和國公共安全行業標準 GA/T 756-2008 數字化設備證據數據發現提取固定方法, 2008
[31] 中華人民共和國公安部, 中華人民共和國公共安全行業標準 GA/T 825-2009 電子物證數據搜索檢驗技術規範, 2009
[32] 中華人民共和國公安部, 中華人民共和國公共安全行業標準 GA/T 826-2009 電子物證數據恢復檢驗技術規範, 2009