數位鑑識機構認證標準規範及操作程序之介紹與建議

陳受湛[1] 林怡伶[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]m43040@mjib.gov.tw [3]chiahwu@deloitte.com.tw
[4]lsung@deloitte.com.tw

摘要

建立數位鑑識標準規範是政府推行數位鑑識產業發展之重要基石，基於我國為大陸法系之司法判決方式，唯有一致性規範標準的產生，才能使公部門或有意從事數位鑑識服務之民間機構，其技術產出證據成果能於司法檢視下而不受質疑。本報告之研究目的係透過調查局資安鑑識實驗室申請 ISO/IEC 17025 之實務經驗，發展適用於數位鑑識機構的認證體系、證物處理標準作業程序與能力評核標準，使鑑識機構之設立運行有所依歸；並結合前述之研究成果，以期作為數位鑑識認證標準規範之推行依據。

關鍵詞：數位鑑識機構認證、數位證物處理標準作業程序、數位鑑識產業能力評核

壹、前言

數位鑑識在台灣之研究發展自 2000 年起始有蔡震榮與張維平兩位學者提出學術成果發表[18]，此後社會各界對於數位鑑識之觀感印象，仍停留在檢調與軍警等公部門所採用的電腦相關調查手法。由於技術面的背景門檻與數位資料的特殊性，數位證據在實際訴訟攻防情境中，過去從未被社會大眾所特別重視。直至 2010 年起個人資料保護法之公佈，其中涵蓋對於個資侵害事件的查明及舉證責任要求，方使得社會各界紛紛關注起數位鑑識領域在刑事甚至民事案件求償上可扮演的角色[17]。

由於數位證據本身的脆弱特性[9]，加上”證據”在司法訴訟中往往為影響當事人受判決裁定的關鍵點，Jordaan[6]在研究中指出，若缺乏適用於數位證物處理過程的一致性品質確保方法，將造成調查成果在法庭訴訟不被信任，甚至可能導致有罪者釋放及無辜者定罪等風險。而英國下議會科技委員會[10]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。由此可推論，數位鑑識領域同樣必須建立對應之標準化規範，方可確保數位鑑識技術與其成果為社會各界與國際認可。

目前政府並無針對數位鑑識領域制定標準化規範，雖有國內學者提出不同流派的數

位鑑識程序學說，但未曾出現一致性共識。有鑑於此，本研究將以國際 ISO/IEC 17025 實驗室認證為研究主軸，結合協助調查局資安鑑識實驗室認證之經驗，以國際要求之規格研擬數位鑑識機構之認證規範，及數位鑑識標準操作程序，並能做為政府機關檢測數位鑑識機構能力之評核標準。

本研究報告在研究架構、研究方法上，力求專業與完整，在資料蒐集上力求充分詳實，但有其限制與範圍如下述：於證物相關操作程序方面，因 ISO/IEC 17025 僅針對實驗室範圍內之證物處理過程（包含證物管理、分析與報告出具）進行規範，但本研究要求涵蓋證物之保全與運送範圍，因此就此二類處理過程則參照 ISO/IEC 27037 數位證據識別、蒐集、擷取與保存指引之內容進行操作程序之規劃。另於產業成熟度能力評核方面，因國際間有發展數位鑑識能力評核之國家或組織相對較少，本研究僅能針對美國與中國大陸兩國現況進行研究。

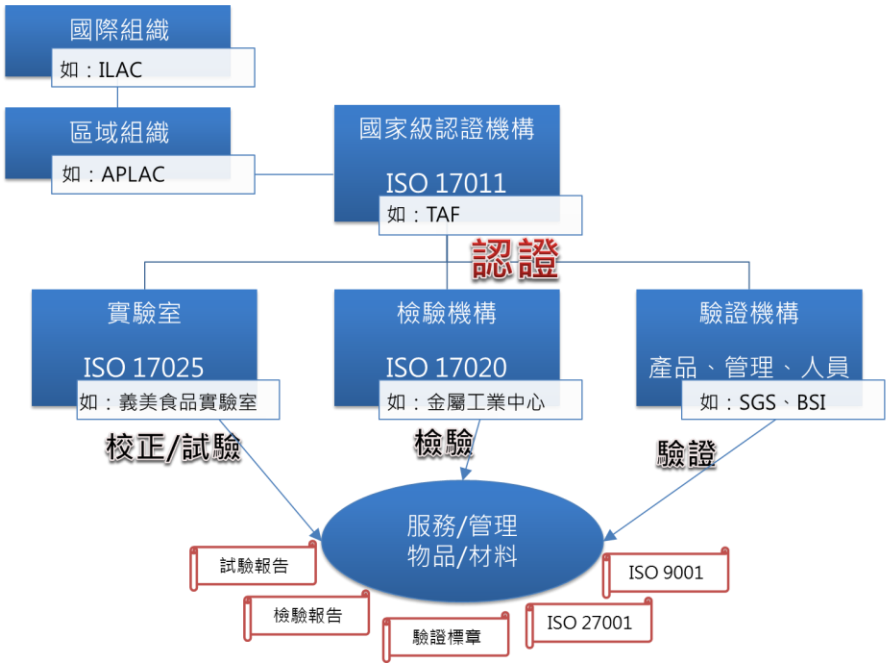
貳、 文獻探討

一、鑑識機構認證制度

國際間現行之符合性評鑑機構認證對象可分為實驗室、檢驗機構及驗證機構（包含產品驗證、品質與環境管理驗證及人員驗證），其整體關係圖可參照圖一，各國有專屬之國家級認證機構，且參與認證體系的區域性/國際性組織，使其授予認證於國際間有相互承認之效果。而認證機構本身需符合 ISO 17011 之國際標準，其認證對象實驗室則需符合 ISO 17025 之國際標準（另有特殊領域如醫學實驗室則另需符合 ISO 15189），且實驗室若以鑑識科學檢驗為目的者，受評鑑時需一併符合鑑識科學實驗室認證技術規範[4]；依據被認證機構之類型不同， 而可對一般物品/材料或管理/服務等，進行具備權威公信力之檢測、檢驗或驗證等專業服務，受驗標的也能藉此證明其合格性、品質水準或取得公正性之結果報告。

2003 年時，經濟部標檢局將國內相關認證體系機構整併為「財團法人全國認證基金會」（Taiwan Accreditation；TAF），自此 TAF 成為我國唯一專責之認證機構，並負責統籌管理全國性認證事宜;於現階段依舊為亞太實驗室認證聯盟(Asia Pacific Laboratory Accreditation Cooperation ； APLAC) 及國際實驗室認證聯盟(International Laboratory Accreditation Cooperation，ILAC)具備相互承認協定之成員。

有鑑於科學技術之發展，普遍使用之數位設備所蘊藏證據在司法訴訟中佔據比例已開始穩定成長，肩負出具數位鑑識報告職責之實驗室將扮演關鍵之角色；由於數位鑑識相對於其他學科是較為新穎及在國內無具體規範之領域，且數位鑑識檢驗分析之品質結果將影響司法訴訟之判決與大眾之安全與公平體認，故實驗室之運作與管理確實需加以嚴格監督。而取得認證是國際間公認作為品質監督之良好方式，透過公正單位的評鑑，可以讓公眾得知兼具完善管理制度與技術能力之數位鑑識機構，以確保品質把關之成果。



圖一 ：認證體系關係圖

二、能力評核機制探討

美國鑑識科學實驗室主管學會/實驗室認證委員會認為，能力試驗是驗證實驗室技術程序與品質維護之可靠方法**錯誤! 找不到參照來源。**。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評核，才具有較佳之一致性基礎。現行國際間所參照之能力試驗設計機制皆依循 ISO/IEC 17043**錯誤! 找不到參照來源。**實驗室間比對之能力試驗指引，以下就該指引所提及之評核機制進行概述：

（一）測量比較法

或稱為單一物質測試法，由同一個物質，在不同實驗室之間輪流試驗。

（二）實驗室間測試法

先同時將相同之樣本集合配送至所有參與實驗室，再隨機選擇樣本子集合。請參與實驗室對樣本子集合加以試驗，並將試驗結果回報與審核單位。由審核單位將各參與實驗室回報之結果與設定值做比較，以給出個別參與實驗室以及整體之能力評核指標。

（三）樣本分離測試法

將一個樣本分為兩部分，分予二個不同之參與實驗室，並保留一份樣本予協力廠商實驗室以為參與實驗室出現試驗結果重大差異時仲裁之用。與其他方法不同之處在於此方法常用於參與實驗室較少(通常只有兩個)時。通常用於識別較低精準度；描述一致性的偏差；驗證矯正措施之有效性。

（四）定性法

此方法無須與其他實驗室進行比較，可用於測試參與實驗室是否有能力識別測試物質之某項特徵(如：石棉之類型；識別病原體)。此方法乃由統籌機構特別準備測試物質，且此測試物質必須具備欲請參與實驗室識別出之特徵。

（五）已知值法

預先準備已知量之測試物質，用以測試參與實驗室是否有能力對該物質進行試驗並提供數字結果與設定值相比較。此方法同樣也無須多個實驗室同時進行。

（六）部分程序法

此方法僅為測試參與實驗室執行試驗或測量之部分程序。如：將給定之資料集預以轉化(transform)或報告(report)；或製作給定規格之樣本。

（七）持續性測驗

定期提供測試物質予實驗室以測試其能力。

（八）一次性試題

於同一處所，參與實驗室使用同一個測試物質進行試驗。

參、數位鑑識認證標準規範及操作程序國際現況

一、鑑識機構認證規範現況

（一） 英國

英國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。2009 年，英國國內事務部(Home Office)轄下之鑑識科學監管局(Forensic Science Regulator)的研究有關鑑識執業者認證方式，向各方專家諮詢所蒐集的回應意見中指出，所有具備實驗室功能（如映像檔製作）的鑑識服務提供者，都應認證 ISO 17025；甚至包含為軍方或執法機關內部服務之單位**錯誤! 找不到參照來源。**；這也表示雖然部分單位已明確具備國家公權力之象徵，但同樣應受到品質系統之評鑑檢視，以確保鑑識分析之成果報告出具於法庭之可信度。

該局又於 2012 年提出「實務與行為守則之附錄[3]**錯誤! 找不到參照來源。**：數位鑑識服務」諮詢草案以蒐集各方意見，並針對部分特定關於數位鑑識之條款提供進一步說明；當中載明所有提供者除遵循前述之「實務與行為守則」一切要求外，有任何犯罪現場活動者，應認證 ISO 17020 檢驗機構認證規範；而有任何實驗室功能者(如：電子資料的映像檔製作或復原等處理證物相關者)，應認證 ISO17025 實驗室認證規範。

（二） 美國

美國最具規模鑑識機構為聯邦調查局(FBI)於各地之實驗室，FBI 也是美國鑑識發展的重要推手；於 1973 年領導成立[7]，但在 1988 最終成為對外服務之非營利組織的美國刑事鑑識實驗室主管協會/認證委員會 ASCLD / LAB(American Society of Crime Laboratory Directors / Laboratory Accreditation Board)，該協會發展出一套專屬之品質認證標準。

1995 年，ASCLD 成立國家鑑識科學技術中心 NFSTC(National Forensic Science Technology Center)負責協助鑑識實驗室準備 ASCLD / LAB 認證，並基於接軌 ISO 17025 立場，而成為獨立認證單位 FQS(Forensic Quality Service)。ASCLD / LAB 在 2003 年通過採用 ISO 17025 為認證標準，並將原有 ASCLD/LAB 認證要求修訂為 ASCLD/LAB-International Testing Laboratories: 2011 Supplemental，亦針對適用於鑑識科學領域之 ISO 17025 條款加以補充要求。

FBI 實驗室與重要鑑識社群 SWGs (Scientific Working Groups)長期具有工作夥伴與贊助關係，SWGs 負責產出特定鑑識領域之指引手冊與標準提供 FBI 做知識參考。該組織於數位鑑識領域之長期研究小組 SWGDE(Digital Evidence)於 2012 年提出一份最新版品質保證手冊予數位證據實驗室作為參考[11]，其內容是採用 ISO 17025 與 ASCLD/LAB Supplemental 之認證規範，並針對部分數位鑑識特定要求進行細部說明，為數位鑑識實驗室運作之主要參考依據。

（三） 中國大陸

中國大陸之鑑識機構發展與國家層級有密切相關，從 1994 開始之國家級實驗室認證（中國大陸原文為：認可）機構成立[13]，至 2006 年將全國認證機構整合為單一由中國國家驗證（中國大陸原文為：認證）認證監督管理委員會 CNCA 所授權之中國合格評定國家認證委員會 CNAS，由該組織主責國內 ISO 體系評鑑，如 ISO 17025(檢測和校準實驗室能力認證準則)；並在 2010 年發佈「檢測和校準實驗室能力認證準則在電子物證檢驗領域的應用說明」，針對 ISO 17025 適用於數位鑑識領域的章節做出額外說明。

而 CNAS 於 2011 年頒佈了實驗室認證領域分類[12]，將電子物證再做細化區分；並於 2013 年 5 月發佈新 CNAS 標準草案「司法鑒定/法庭科學機構能力認證準則」，擷取 ISO 17025 與 ISO 17020 的章節精神，並預計於後續發佈適用於特定領域的應用說明。

（四） 台灣

台灣之鑑識機構認證規範發展相對緩慢，雖具有成熟的 ISO 17025 實驗室認證體系，但針對鑑識領域之細部說明，僅有參照 ILAC 於 2001 年提出的鑑識科學實驗室認證技術規範[16]。而國內對於數位鑑識機構之品質認證推動也尚未有一致性規範出現。而類似性質之檢驗機構則有「政府機關濫用藥物尿液檢驗實驗室設置標準」與「濫用藥

物尿液檢驗及醫療機構認可管理辦法」[14]及其相關作業準則，亦是參考 ISO 17025 之精神而制定。

（五） 綜合觀點比較

由以上各地之鑑識機構認證規範進行分析比較，可知國際上對於鑑識機構認證發展最早為美國，也擁有專門鑑識實驗室認證規範，但因 ISO 體系在國際間廣為接受，最終和英國一樣，以 ISO 17025 作為鑑識機構之主要標準規範，並因應實際現況發展出針對特殊領域之補充說明內容。至於中國，在保持 ISO 認證外，則是另行彈性設計國內專屬資質認定，讓不同規模之鑑識機構同樣能依照 ISO 17025 之精神運作。

以下將對於鑑識認證規範中，對於數位鑑識領域之要求，進行「人員」、「環境設施」、「作業程序」與「工具驗證」方面的特色比較，並以清單方式呈現；惟因台灣並無數位鑑識領域認證規範，暫以濫用藥物尿液檢驗相關要求一同加入比較：

表一：鑑識機構人員資格

國家/規範	**實驗室認證鑑識人員資格**
國際/ ISO 17025	➢ 應定義明確人員能力要求（包含教育、訓練、經驗與實作），且確認任職人員都能符合
英國/ 實務與行為守則	➢ 依循 ISO 17025 要求
美國/ 數位證物實驗室品質保證手冊	➢ 依循 ISO 17025 要求 ➢ 技術人員應符合職務之教育背景，至少為理學士 ➢ 技術人員於特殊領域需有證照要求 ➢ 負責報告解釋人員應有足夠訓練、經驗與檢驗知識
中國大陸/ 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	➢ 依循 ISO 17025 ➢ 從事電子物證檢驗技術人員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。 ➢ 電子物證實驗室授權簽字人應在本專業工作 5 年以上，或具有本專業高級技術職稱。
台灣/ 濫用藥物尿液檢驗及醫療機構認可管	➢ 檢驗負責人應具備下列資格條件之一： 一、具有博士學位，主修分析化學或其他相關之自然科學，且具一年以上之實務經驗。

理辦法	二、具有碩士學位，其大專或研究所主修分析化學或其他相關之自然科學 ，且具三年以上之實務經驗。 三、大學或專科學校化學或其他相關自然科學之科系畢業，且具五年以上之實務經驗。 ➢ 專責品管人員應具備下列資格條件之一： 一、具有博士學位，主修分析化學或其他相關之自然科學，且具一年以上之檢驗實務經驗。 二、具有碩士學位，其大專或研究所主修分析化學或其他相關之自然科學 ，且具二年以上之檢驗實務經驗。 三、大學或專科學校化學或其他相關自然科學之科系畢業，且具三年以上之檢驗實務經驗。 ➢ 人員應受有相當之訓練，並具所擔任工作必備之技術。

表二：鑑識環境設施之要求

國家/規範	**環境設施**
國際/ ISO 17025	➢ 實驗室設施，包括但不限於能源、照明及環境條件，應有助於試驗的正確執行，且不會造成檢驗結果無效。 ➢ 會影響試驗與校正結果的設施與環境條件之技術要求，應予書面化。 ➢ 鑑識科學實驗室在分析或測定微量物質包括 DNA 時，須有特別考量。對不同環境監控要求的工作空間需予以隔離。專屬空間的進出與對其內工作須加以管制，並保有適當記錄證明管制效果。實驗室可能也須對執行之儀器、工作場所、衣物與耗材的環境條件進行監控。 ➢ 實驗室的工作區須有管制與限制。進入實驗室工作區訪客須有限制與記錄。 ➢ 證物儲存區應有進出管制與安全措施以防竊或干擾。儲存條件須足以防止遺失、腐敗與污染，及確保證物的完整與標示，這些管制條件執行適用於檢驗前後程序中。

英國/ 實務與行為守則	➢ 依循 ISO 17025 要求 （適當時，實驗室應具有以下條件：） ➢ 合適實驗室設施、家電及個人空間，以便於遵循標準且安全地不造成交叉污染 ➢ 適當環境條件(如溫溼照明)使設備能有正確檢驗結果，且不會影響結果品質 ➢ 符合比例原則的保護，免於如縱火、竊盜或干擾證物等風險 ➢ 有適當儲存條件的歸檔/儲存設施，以防止遺失、變質與污染，且無論是在檢驗或試驗前後，都能保持檔案/紀錄/證物的完整性與識別性 ➢ 可安全棄置機密內容或處置有害材料的設備 ➢ 證物儲存區域、伺服器間的進入與使用，與實驗室工作區同樣都應該受到管制。提供者應持有授權進入區域的員工列表，並定期檢視與更新 ➢ 運送與卸貨區，或其他未授權人員可進入區域，應與案件工作/資訊處理區域隔離及管制。未授權人員欲進入管制區時，應有員工全程陪同與登記進入情形。 ➢ 建議遵循 ISO 27001 與 27002 資訊安全要求
美國/ 數位證物實驗室品質保證手冊	➢ 依循 ISO 17025 要求
中國大陸/ 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	➢ 依循 ISO 17025 ➢ 電子物證檢驗實驗室的地面應鋪設防靜電地板，對手機檢驗應具有手機信號遮罩設施。 ➢ 電子物證檢驗實驗室應具備保護其資訊網路安全的措施，包括防範電腦病毒等惡意程序碼、防範網路入侵的措施。 ➢ 在影響檢驗結果的軟體升級時應記錄軟體的名稱和升級後的版本號。
台灣/ 濫用藥物尿液檢驗及醫療機構認可管理辦法	➢ 設施應符合相關法令規定。電器設備應適當接地，並應有抽氣櫃、滅火器、緊急淋浴設備、洗眼裝置及其他保障檢驗人員之安全設施 ➢ 水電、照明、溫溼度、空間規劃、設備與安全性及其他環境條件，應符合檢驗需求，對於影響檢驗結果之環境因數應加以監測並記錄之 ➢ 應有隔離管制之尿液檢體儲存區、檢驗區及紀錄儲存區

表三：鑑識作業程序之要求

國家/規範	**作業程序要求**
國際/ ISO 17025	➢ 所有方法都須有完整的書面敘述。 ➢ 鑑識科學實驗室使用之技術程序，在應用於案件前都須經過確認有效。 ➢ 當實驗室使用新的（或已確認）方法時，須針對該程序所有書面記載的效能特性，在實驗室內證明其可靠性。 ➢ 效能查驗的紀錄應予維持以供未來參考。 ➢ 當顧客未指明採用方法時，實驗室應選擇國際的、區域的或國家標準，或著名的技術組織、相關科學書籍或期刊所發行的適當方法，或設備製造商所指定的適當方法。
英國/ 實務與行為守則	➢ 依循 ISO 17025 要求
美國/ 數位證物實驗室品質保證手冊	➢ 依循 ISO 17025 要求
中國大陸/ 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	➢ 依循 ISO 17025 ➢ 實驗室應按照相關的檢驗技術規範進行電子物證檢驗，包括檢驗環境、檢驗工具、檢驗步驟及其檢驗結果的描述；檢驗樣品的提取、封裝、保存、對樣品的各個功能的檢驗所採用的檢驗方法順序及檢驗方法的組合等。
台灣/ 濫用藥物尿液檢驗及醫療機構認可管理辦法	➢ 應訂定檢驗所需各項儀器之操作、維修及校正標準作業程序，以及其相關執行紀錄。

表四：鑑識工具驗證之要求

國家/規範	**鑑識工具驗證**
國際/ ISO 17025	➢ 鑑識科學實驗室使用的所有技術程序，在應用於實際案件前，都應經過「確認」。 ➢ 「確認」研究，可以由科學團體來實施（如標準方法或已發表方法），或由鑑識科學實驗室本身進行（如由本身所發展出的方法或就先前已確認的方法，進行有顯著的改變）。

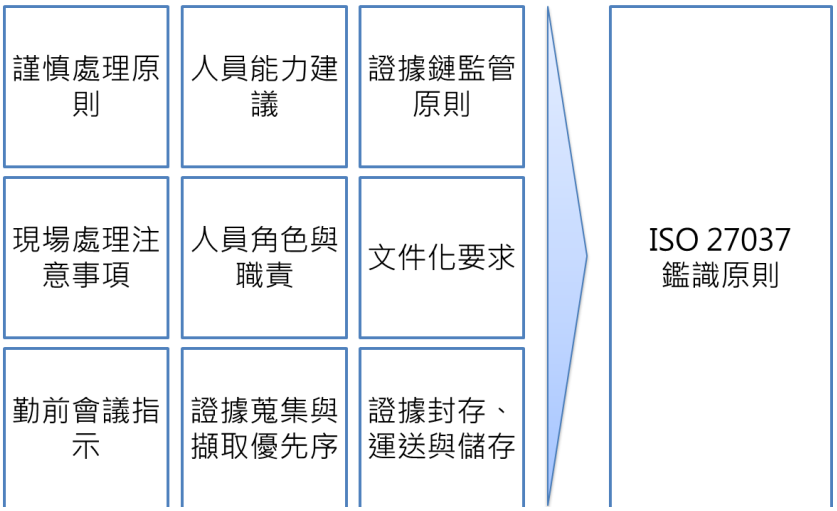
	➢ 實驗室應對非標準方法、實驗室設計/開發之方法、使用上超出其所預期範圍的標準方法及標準方法的擴充與修改加以確認，以證實這些方法適合所預期用途。確認應依所需加以延伸，以符合預定應用或應用領域的需求。實驗室應記錄所獲得的結果、確認所用的程序及方法是否適合所預期用途的陳述。
英國/ 實務與行為守則	➢ 依循 ISO 17025 要求 ➢ 凡是其操作對取得結果有影響之軟體、硬體與軟體工具，都要求確認，或將任何現有確認做驗證 ➢ 提供者應確保，在各種類型的數位鑑識工具使用時，驗證要求應考量員工能力等級、該執行工作的特性與困難性，以及該工具在廣大鑑識科學與刑事社群的接受程度。
美國/ 數位證物實驗室品質保證手冊	➢ 依循 ISO 17025 要求 ➢ 若有效性研究已由 NIST 進行，或其他組織已實行有效性研究；至少，應進行核對與載明證實該裝置與我方軟硬體設定為相容有效。
中國大陸/ 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	➢ 依循 ISO 17025 ➢ 實驗室自行制定檢驗規範應通過聘請3名以上具備高級職稱的外部專家進行確認，確保其可行性、有效性和結果重複性、複現性的要求。
台灣/ 濫用藥物尿液檢驗及醫療機構認可管理辦法	➢ 應訂定天平、溫度計、移液管、定量瓶等量測設備之校正作業程序，明定校正方法、校正頻率、合格範圍，以及不合格之限制使用及修正措施。

二、證物相關標準操作程序現況

現今與數位證據蒐扣現場相關的國際標準仍為少數，直至 2012 年才有現場證據保全的國際規範 ISO/IEC 27037 被發佈，至於證物送入數位鑑識實驗室後之處理過程，已有發展歷史悠久的 ISO/IEC 17025 實驗室規範可依循。此章節分別探討其要點如下：

（一） ISO/IEC 27037

ISO 27037 是一份數位證據現場操作指引，針對數位證據的識別、蒐集、擷取與保存各個任務進行說明，分別為以九大鑑識原則為主軸：



圖二：ISO/IEC 27037鑑識原則

1. 謹慎處理原則：由於數位證據擁有易遭改變、毀損、破壞與易被時間影響[8]之特性，故在處理上亦必要格外地強調數位證據之完整性，以保全其證據能力。
2. 人員能力建議：由於數位證據之蒐集、分析過程皆有可能導致原始資料之改變(如 1.所述之特性)，故當須存取原始資料時，應確保人員之能力足以實作且可以說明即將進行之行為與證據之關聯性為何[1]。
3. 證據鏈監管原則：如 1.所述之特性，數位證據之處理過程中之每一道程序皆應被完整記錄下來(即證據監管鏈[8])。以備協力廠商得以依據留存之紀錄重現程序並得到相同的結果[1]。如此以驗證數位證據之正確。
4. 現場處理注意事項：為保持現場之完整，該規範要求應設置現場管制負責人以確保管制現場進出與證據之存取，除隔離嫌疑人員與現場的接觸外，並應記錄現場環境與設備狀態，並管制設備現況與相關資訊等。
5. 角色與職責：ISO/IEC 27037 該標準規範將涉及數位鑑識證據保全作業程序之人員分為兩種角色，其一是數位證據一線應變人員，主要職責為數位證據辨識、蒐集、擷取與保存，包含數位證據蒐集及擷取報告內容編列、數位證據保存及處理；其二是數位證據鑑識專家，具備專業鑑識職能，主要在一線人員面臨無法處理情形時，提供技術性協助，例如複雜之伺服器架構、磁碟陣列儲存裝置等。
6. 文件化要求：要求詳細記錄操作動作與所存取之資料名稱、螢幕顯示畫面、目標設備之廠牌、型號、規格等資訊，並建議可用攝影方式記錄。
7. 勤前會議指示：由於進行證據保全時，現場環境情況可能無法預料，因此必須先透過勤前會議說明案情方向、處理證據類型、人員職責分工、異常狀況處理對策等。
8. 證據蒐集與擷取優先序：若電腦主機是開機狀態，則非必要時不要關閉電腦主

機。揮發性資料，如 RAM、Cache RAM、Register、主機正在執行中的程序、網路連線與應用程序開啟通訊埠等，可能因關閉主機而資料就此消逝無法回復。

9. 證據封存、運送及儲存：在證據取得完畢後，在證據封存時應有明確標示記錄與阻隔防護性包裝；在證據運送過程中應處於受到監管與保護之環境；最終於證據儲存地點，應確保實體與防護之安全性。

（二） ISO/IEC 17025

此份規範為實驗室認證之通用性規範，不論何種領域實驗室，在其管理面與技術面要求都能依循做法，以達成且維持實驗室的品質水準；然而在各領域技術的差異性考量下，ISO 國際組織也針對部分技術領域發佈專門適用的補充性技術規範（如鑑識科學技術規範）。

ISO 17025 說明對整體實驗的運作規範要求，其中也有數個章節可對應至數位證據的管理、分析與報告出具，分別討論於其下：

1. 證物（試驗件）之處理：在證物的管理方面，ISO 17025 之要求為證物的運輸、接收、處理、防護、儲存、保留及清理等過程，都能確保完整性與安全性的維持，此外，補充技術規範亦特別要求證物監管鏈之維持與證物的監控管制。
2. 試驗分析方法：試驗分析方法是實驗室品質的技術展示關鍵，所採用的分析方法是否皆做成書面記載，並經過確認為有效方法，並持續定期查驗該分析方法的有效性，才能確保實驗室的分析產出成果之品質與可靠性。
3. 分析結果之品質保證與報告出具：在實驗室的成果品質的檢驗上，透過其他人員與管理層級的查核，可確保出具內容的品質；而在報告出具的內容要求方面，對於分析單位、委託單位、分析標的、結果、使用方法與其他解釋等，都應明確的揭露於報告之中。

三、數位鑑識產業能力成熟之評核標準現況

在數位鑑識實驗室的認證規範中，技術面的呈現與證明也被視為為實驗室維繫作業品質之必要考量因素之一；因此在實務評鑑時，除了管理文件的審核外，針對整體技術能力的實作展現也會同樣受到嚴謹的考核檢視。

唯有具體發佈的測試方法，對於能力成熟度才會有一致性的評核標準，例如實驗室認證體系中要求的能力試驗，即是最佳範例；依據 TAF 組織之定義[15]，能力試驗為：透過實驗室間比對並依照既定的標準來判斷實驗室的技術。然而現行國際間對於數位鑑識領域專屬的技術方法著墨不多，以下就美國與中國大陸的發展現況進行說明：

（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[2]，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之技術能力水準。

（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，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標準檢驗方法之官方依據。

肆、研究規劃與結果

一、數位鑑識認證標準規範之規劃建議

數位鑑識機構認證規範之建立目的為確保鑑識分析成果品質，對大眾而言能保護其司法訴訟中之權益；對政府機關而言，可以協助認可數位鑑識機構之能力品質；對有志發展數位鑑識實驗室之公部門或私人機構，能有一個具體規範可明確依循認證。

數位鑑識認證規範架構內容牽涉範圍相當廣泛，包括組織、管理系統、試驗收件審查、採購、文件與紀錄管制、人員、環境設施、試驗方法及確認、設備、試驗件處理、試驗品質保證與結果報告等項目。如本文前言所述，為確保數位鑑識技術與其成果為社會各界與國際認可，本研究範圍將以數位鑑識機構認證過程中，涉及技術面架構重要要求為主，包括鑑識人員資格、環境設施、作業程序、鑑識工具驗證等為主要研擬項目。

經綜合前述國內外鑑識機構認證規範之特色，參照現行與 TAF 認證服務計畫已接軌之我國法定他類實驗室認證規範[19]為設計框架，並歸納經由研討會而取得之各界建言後，本研究提出以下初步規劃擬定之認證規範：

表五：數位鑑識機構認證標準規範建議

第一章 鑑識人員設置

第 1 條

數位鑑識實驗室(以下簡稱實驗室)應設置實驗室主管、品質主管、報告簽署人及鑑識分析人員等。

前項實驗室之專職人員應不得少於三人，當試驗類別二項以上時，其專職人員應不得少於四人。

實驗室主管、品質主管或報告簽署人，應具有下列資格之一：

1. 國內外大學以上學校理工資訊相關科系畢業，並具實際數位鑑識工作經驗共三年以上者。
2. 國內外研究院所資訊相關院所畢業得有碩士學位，並具實際數位鑑識工作經驗共二年以上者。
3. 國內外研究院所資訊相關院所畢業得有博士學位，並具實際數位鑑識工作經驗共一年以上者。

品質主管，除前項資格外，另應具有下列資格之一：

1. 受過實驗室品質系統之相關訓練合格者。
2. 曾經參與實驗室內部稽核相關訓練合格者。

鑑識分析人員，應具有下列資格：

1. 國內外大學以上學校理工資訊相關科系畢業，並取得數位鑑識專業訓練課程結業證明者。
2. 國內外研究院所資訊相關院所畢業得有碩士以上學位，並曾修習數位鑑識專業學科取得學分者。

第 2 條

有關實驗室人員之訓練，應符合下列規定：

1. 新進及新派任員工之訓練，應包括儀器設備、品保品管及分析技術三大部分，各部分應有計畫及執行之紀錄。紀錄應至少包括訓練項目、訓練方式、訓練期程、訓練人員及訓練成果等。
2. 實驗室每年應進行人員訓練，鑑識分析人員應每年評估其能力。
3. 實驗室人員應參加適用之各種實驗室相關講習會、研討會或訓練。
4. 每人每年訓練時數至少十二小時。

第二章 作業程序

第 3 條

實驗室之試驗方法原則如下：

數位鑑識機構應訂定鑑識試驗分析所需各項儀器之操作、維護及查核標準作業程序，以及其相關執行紀錄。

實驗室應按照相關的試驗分析技術規範進行數位鑑識試驗分析，包括試驗工具、試驗步驟及其試驗結果的描述；試驗目標證物的取出、封裝、保存、對證物的各類試驗分析所

採用的試驗方法順序及試驗方法的組合等。
應參考國際間著名數位鑑識相關技術組織、相關科學書籍或期刊所發行的適當方法，或設備製造商所指定的適當方法所發佈之標準方法。

第三章 鑑識工具及方法驗證
第 4 條
實驗室工具及方法確認原則如下：
凡是其操作對取得結果有影響之軟體、硬體與軟體工具，都要求確認，或將任何現有確認做驗證，並留下相關紀錄。
若有效性確認研究已由外部國際知名數位鑑識相關技術組織（如：NIST、SWGDE 等）實行過，應進行檢核證實該裝置與我方軟硬體設定為相容有效。
當實驗室使用新的（或已確認）方法時，須針對該程序所有書面記載的效能特性，在實驗室內證明其可靠性。

第四章 環境設施
第 5 條
實驗室之環境與設施，應符合下列規定：
實驗室之一般性要求應包含下列事項：
1. 設施以及環境條件應當滿足相關法律法規、技術規範或者標準的要求。
2. 電力、網路、照明、溫溼度、空間設置、設備與安全性之規劃，不得對鑑識分析結果造成影響，並滿足設備運行需求。

實驗室之實體環境控管應包含下列事項：
1. 實驗室之工作區域、證物儲存區與伺服器機房應有門禁管制，進入訪客須留下紀錄證明，且應有實驗室人員全程陪同。
2. 應有適當歸檔/儲存設施，須足以防止遺失、變質與污染，及確保檔案/紀錄/證物的完整與標示。
3. 應維持授權進入管制區域的人員列表，並定期檢視與更新。

實驗室之資訊環境控管應包含下列事項：
1. 運行鑑識分析之主機應與連線網際網路環境進行實體隔離。
2. 在使用鑑識試驗分析結果的軟體時，應維持相關紀錄並確認為最新有效版本。

實驗室之環境監測，應達下列規定：
1. 各種電氣設備應定期維護、保養。
2. 消防設施應依消防法規定期檢查，並確保其性能。

實驗室之廢棄物，應達下列規定：
1. 包含顧客或實驗室資訊之欲廢棄紙本，應於核准後以碎紙機銷燬，並留存紀錄。
2. 包含顧客或實驗室資訊之欲報廢儲存媒體，應以資料不可回復方式進行物理/電磁類破壞性報廢；且於報廢進行前，應暫置於上鎖空間存放。

二、數位鑑識標準操作程序之規劃建議

數位證據之保全主要針對蒐扣現場之證物進行處理，這其中又包含了前置準備、識別、擷取、蒐集與封存等工作，結合運送程序將證物完整妥善取回。

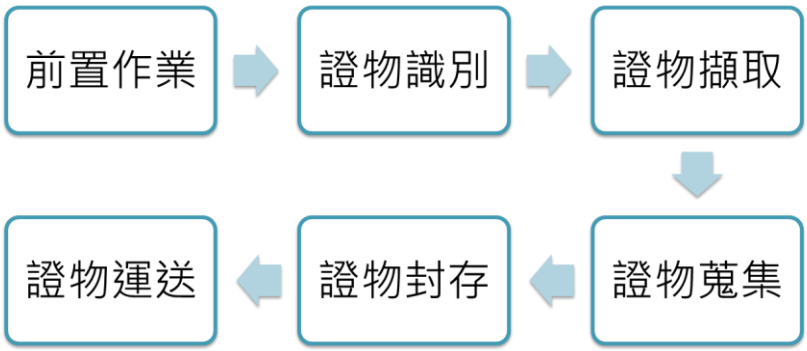


圖 三：數位證物保全與運送程序

在數位證據管理時所涉及的實務作業內容為，實驗室對於證物的收件與出入庫監管；而為符合 ISO 品質精神要求，分析後之成果報告需經過品質審查且符合撰寫要求，故將操作項目再行細分如下：

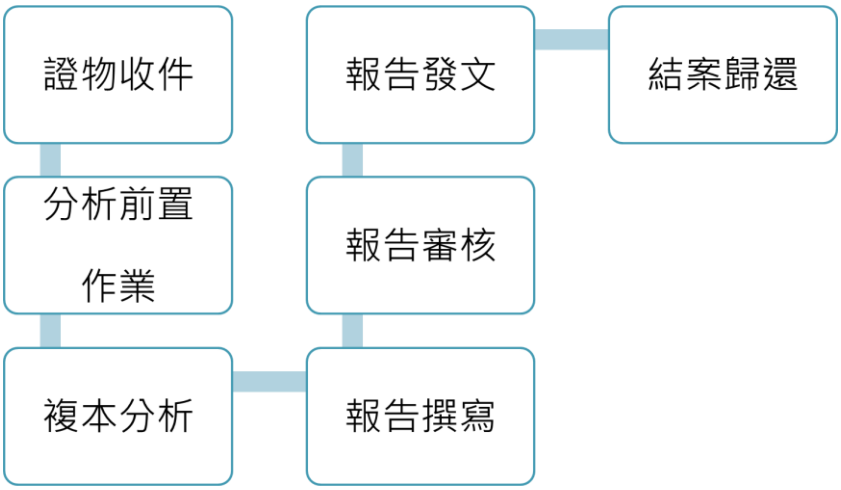


圖 四：數位證物管理、分析與報告出具程序

數位鑑識技術能力之試驗方法有其特殊性，依據 ISO/IEC 能力試驗導引與要求之原則判定，數位鑑識技術能力之測試方法屬於定性分析，且其技術能力之審核方法以審核專家之共識意見為其典型評估方法。而本研究將分別就「資料回復」與「資料搜尋」兩種技術能力試驗方法，提出通用性能力評核標準之實務規劃建議。

（一） 進行資料回復時，應在不變動原始儲存媒體之前提下，利用鑑識工具針對儲存媒體之被刪除內容進行復原。還原後之檔案須與原始檔案完全相同。其能力評核過程如下：

1. 審核單位之試驗件準備
   (1) 將作業系統安裝於經硬碟抹除後之儲存媒體 A。
   (2) 將欲回復之標的檔案儲存於儲存媒體 A 之作業系統中。
   (3) 將標的檔以 Del 指令刪除(以 Windows 環境為例)後拔除電源。
   (4) 以磁碟複製機計算儲存媒體 A 之雜湊值。
   (5) 將儲存媒體 A 做鏡像複製於經硬碟抹除後之儲存媒體 B(容量需大於 A)。
   (6) 比對確認儲存媒體 A 與儲存媒體 B 之雜湊值相同。
   (7) 使用磁碟防寫設備連接儲存媒體 A 後進行標的資料回復，記錄所得之標的檔案雜湊值（此為設定值）。
   (8) 將儲存媒體 B 封存後運送至受測單位作為試驗件。
2. 受測單位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)。
3. 準備試驗所需設備（包含硬體設備與儲存媒體之設置）。
4. 執行與記錄試驗技術項目（包含攝影與書面）。
   (1) 將審核單位提供做為試驗件之儲存媒體 B 進行雜湊值計算。
   (2) 對儲存媒體 B 進行鏡像複製到儲存媒體 C。(容量大於或等於儲存媒體 B，且複製後儲存媒體 C 之雜湊值應與儲存媒體 B 之雜湊值相等。)
   (3) 以磁碟防寫設備連接儲存媒體 C 並依照審核單位給定之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其雜湊值。
   (5) 此檔案雜湊值與該復原所得檔案即為應回傳予審核單位之結果。
5. 進行試驗結果封存（包含雜湊值與檔案等）。
6. 進行結果紀錄封存（包含影音檔或儲存媒體）。
7. 試驗結果提供予審核單位（包含書面報告與影音檔等）。

（二） 進行資料搜尋時，應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搜尋指定關鍵字，其搜尋範圍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。其能力評核過程如下：

1. 審核單位之試驗件準備
   (1) 將作業系統安裝於經硬碟抹除後之儲存媒體 A。
   (2) 將含有搜尋標的之檔案儲存於儲存媒體 A 內之檔案系統中。
   (3) 以磁碟複製機計算儲存媒體 A 之雜湊值。

(4) 將儲存媒體 A 做鏡像複製於經硬碟抹除後之儲存媒體 B(容量需大於 A)。
(5) 比對確認儲存媒體 A 與儲存媒體 B 之雜湊值相同。
(6) 使用磁碟防寫設備連接儲存媒體 A 並以指定關鍵字進行搜尋，記錄存有關鍵字之檔案個數並計算其雜湊值（此為設定值）。
(7) 將儲存媒體 B 封存後運送至受測單位作為試驗件。

2. 受測單位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)。
3. 準備試驗所需設備（包含硬體設備與儲存媒體之設置）。
4. 執行與記錄試驗技術項目（包含攝影與書面）。
(1) 將審核單位提供做為試驗件之儲存媒體 B 進行雜湊值計算。
(2) 對儲存媒體 B 進行硬碟複製得到儲存媒體 C。(容量應大於或等於儲存媒體B,且複製後儲存媒體C之雜湊值應與儲存媒體B之雜湊值相等。)
(3) 將儲存媒體 B 以封存程序進行封存。
(4) 以磁碟防寫設備連接儲存媒體 C 並以審核單位指定之關鍵字進行搜尋。
(5) 計算含有關鍵字之檔案個數並及其雜湊值。
(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。
5. 進行試驗結果封存（包含雜湊值與檔案等）。
6. 進行結果紀錄封存（包含影音檔或儲存媒體）。
7. 試驗結果提供予審核單位（包含書面報告與影音檔等）。

伍、結論與建議

一、結論

數位鑑識機構的認證標準在各國的發展趨勢仍為結合 ISO/IEC 17025 而進行，但各國在順應其國內法律民情之狀況下，皆能逐步發展出專屬適用於數位鑑識領域的衍生規範。對於數位鑑識機構而言，除專業領域的特殊性外，其產出結果影響民眾對訴訟公平公正的期待，也促使該類機構管理走向國家層級的規範要求。

本研究報告之成果如下，可作為各界成立數位鑑識機構之具體認證標準與實務參考規範，以期提昇國內數位鑑識機構之服務水準：

（一） 本研究探究數位鑑識機構較為發達之英、美、中國大陸與台灣， 就其國家標準鑑識機構規範內容進行探討，並研擬出適用於我國數位鑑識機構於「人員資格」、「環境設施」、「作業程序」與「工具驗證」方面之標準規範。

（二） 對於數位鑑識證物處理方面，本研究歸納現行國際規範指引對於現場搜扣證物之要求，以及實驗室標準中所規範證物收件後的處理過程，制定出屬於證物處

理完整生命週期的數位鑑識證物標準操作程序。

（三） 對於數位鑑識產業能力成熟度評核方面，則探究了現行發展較為具體之美國與中國大陸規範，縱理出對於數位鑑識技術評核依據，並依據數位鑑識分析的定性特點，設計出能力評核標準之實務規範建議。

二、建議

本研究報告中所設計之能力試驗機制，係參照 ISO/IEC 17043:2010 能力試驗之一般要求之規定而草擬；於未來由公正主責之評鑑單位（如 TAF 全國認證基金會）帶領發展符合數位鑑識機構之評核方法，亦希冀能將本研究之能力評核研究成果加以採納參考，可發展出符合國際實驗室體系適用之機構能力確認機制。也藉此建立一套檢核數位鑑識實驗室技術能力之機制，進而監督與促使鑑識機構自我保持技術水準，並能持續提供良好鑑識作業品質。

參考文獻

[1] Association of Chief Police Officers, “Good Practice Guide for Digital Evidence”, 2012.

[2] C. D. Faison, J. Horlick, W. R. Merkel, and V. R. White, National Voluntary Laboratory - Accreditation Program Procedures and General Requirements, http://www.nist.gov/pml/wmd/labmetrology/upload/nist-handbook-150.pdf(2006).

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

[4] Forensic Science Regulator, *A Review Of The Options for The Accreditation of Forensic Practitioners*, Crown, 2009.

[5] International Organization for Standardization, *ISO/IEC 17043:2010 Conformity assessment -- General requirements for proficiency testing*, 2010.

[6] J. Jordaan, “A Sample of digital forensic quality assurance in the South African criminal justice system”, *Information Security for South Africa (ISSA)*, pp. 1-7, 2012.

[7] M. E. Schechter, “Ascld/Lab and Forensic Laboratory Accreditation: An Analysis”, *The New York State Commission of Forensic Science*, 2011.

[8] National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition, 2008.

[9] D. L. Shinder, and M. Cross, *Scene of the Cybercrime*, Syngress; 2 edition, 2008.

[10] Science and Technology Committee, *Forensic Science on Trial*, 2004.

[11] Scientific Working Group on Digital Evidence, “SWGDE Model Quality Assurance Manual for Digital Evidence Laboratories”, Version 3, Sep. 2012.

[12] 中國合格評定國家認可委員會，*實驗室認可領域分類*，http://www.cnas.org.cn/sysrk/sysrkgf/lyfldm/images/2012/12/18/182C5D042B4965E65C99BD160A3CE271.doc(2011/8)。

[13] 中國認可的起源與組織體系的歷史沿革，http://www.cnas.org.cn/rdzt/sjrkrzt/zgrkfzlc/2012/05/721462.shtml。

[14] 行政院衛生署，*濫用藥物尿液檢驗作業準則草案總說明*，http://www.doh.gov.tw/ufile/doc/尿檢實驗室作業準則 921014.doc(2004/1/9)。

[15] 財團法人全國認證基金會，*能力試驗活動要求 TAF-CNLA-R05*，2012。

[16] 財團法人全國認證基金會，*鑑識科學實驗室認證技術規範 TAF-CNLA-T11*，2006。

[17] 葉奇鑫、李相臣，“淺談個人資料保護法民事賠償責任及數位鑑識相關問題”，*司法新聲第 101 期* ，2012。

[18] 蔡震榮、張維平，“電腦犯罪證據之研究”，*刑事法雜誌第 44 卷 2 期*，2000，頁 49~63。

[19] 職業衛生實驗室認證規範，http://www.iosh.gov.tw/Law/LawDownload.aspx?K=1&LID=87&F=F3187。