



電腦稽核



Computer Audit Association 民國108年08月30日 第40期

Blockchain-Related Audit Issues

區塊鏈相關之稽核議題

自抹除、刪除與抹除權及被遺忘權

之控制措施的標準化談

「設計及預設的資料防護」：根基於雲端運算服務

Cybersecurity and AI

— Implications for Internal Auditing

Critical Analysis and
Improvement on Block-chain's
Security and Auditing Concerns

銀行業重大裁罰案件
思考建置數位證據鑑識標準

Is BitCoin a reliable
FinTech Tool?

編輯序

在近年來「金融科技」(Fintech)的發展浪潮中，最受到專業人士不間斷發想、討論的科技之一，可說是由傳說中的比特幣(Bitcoin)創辦人「中本聰」(Satoshi Nakamoto)創建的區塊鏈(Blockchain)技術。或許多數人都已聽說過到比特幣如神話般崛起的過程，特別是它保密、去中心化的特質，一度使得它的幣值高達將近 \$ 20,000 美元的匯率。但事實上，區塊鏈才是比特幣創造奇蹟的主要核心技術，從某個角度來看，比特幣可能只是區塊鏈的一項應用而已，由於區塊鏈可以追蹤任何有價值事物的交易，包括股票、債券或其他資產買賣等，它其實具有更大的潛能，可以廣泛應用於比特幣之外的各種交易事件。

繼比特幣而起的以太幣(Ethereum)，便藉著區塊鏈技術成功地推廣了智能合約(smart contract)技術，大大地拓展了區塊鏈的應用空間。智能合約是利用電腦程式碼在合約各方之間闡述、判斷並執行合約中的重要條款，相對於傳統合約以自然語言起草，在智能合約中，條款成為一行行的程式碼，在特定條件被程式判斷為符合時，條款將被自動地執行，並依預定方式影響合約各方的權利與義務；一份複雜的智能合約，更能透過區塊鏈這類無法任意篡改的技術平台進行各種不同資產的交換，例如：股票交割、金融轉帳甚至會計紀錄等。在以太幣創始人 Vitalik Buterin 的理想中，智能合約將成為實踐世界電腦(world computer)的核心工具：所有使用者可將任何交易資料透過智能合約寫入無法任意篡改的區塊鏈網路中。

綜上所述，電腦稽核期刊第四十期以「區塊鏈相關之稽核議題」為主軸，邀請國內外學者與專家，提出具創新性與實用性的論文，剖析區塊鏈環境下所衍生的內部與外部稽核問題，及思考應用現存內控稽核機制來因應相關可能衝擊，為組織、產業、以及政府提出建言。本期收錄文章內容理論和實務並重，包括：「區塊鏈如何影響會計與審計」、「自抹除、刪除與抹除權及被遺忘權之控制措施的標準化談「設計及預設的資料防護」：根基於雲端運算服務」、「Cybersecurity and AI — Implications for Internal Auditing」、「Critical Analysis and Improvement on Block-chain's Security and Auditing Concerns」、「Is BitCoin a reliable FinTech Tool?」、「銀行業重大裁罰案件思考建置數位證據鑑識標準」。希望透過優質文章的收錄，來啟發讀者的關注與研究興趣，進而為資訊治理與電腦稽核領域帶來更成熟之發展。

此期特別邀請美國加州州立大學蒙特利灣分校商學院周濟群教授，擔任第四十期客座主編，共同為電腦稽核期刊帶來更加精采豐富的內容。感謝各位作者賜稿及協會祕書處之協助，更感謝各位審稿委員細心審閱。本期期刊若有不盡之處，敬請各位先進賜教。

張碩毅

編譯出版委員會主任委員
國立中正大學 管理學院院長

周濟群

美國加州州立大學蒙特利灣商學院教授

目 錄

CONTENTS

編輯序

緒論

- 04 區塊鏈如何影響會計與審計
- 周濟群

專業論壇

- 10 自抹除、刪除與抹除權及被遺忘權之控制措施的標準化談
「設計及預設的資料防護」：根基於雲端運算服務
- 蔡昀臻、樊國楨
- 31 Cybersecurity and AI — Implications for Internal Auditing
- Toshifumi TAKADA、Masatoshi SAKAKI、Shiro, AOYAGI、
Hiroshi, KAWAGUCHI
- 49 Critical Analysis and Improvement on Block-chain's
Security and Auditing Concerns
- TSE Woon Kwan Daniel、WANG Yanbing
- 60 銀行業重大裁罰案件思考建置數位證據鑑識標準
- 林宜隆、楊慧茹
- 84 Is BitCoin a reliable FinTech Tool?
- TSE Woon Kwan Daniel、ZHOU Xinquan、CAI Xintong、LI Jingyi、
SHANG Di

會務交流

- 96 協會簡介

- 98 2019 年 09-12 月教育訓練課程
- 101 電腦稽核期刊前期篇名整理
- 102 ISACA 摘譯文章篇名整理
- 103 近期活動整理
- 110 ISACA 國際證照簡介

發行人：張紹斌

總編輯：張碩毅

客座編輯：周濟群

編輯委員：張碩毅、李順保、李興漢、孫嘉明、徐立群、黃劭彥、張益誠、劉其昌、邵之美、
諶家蘭

執行編輯：謝芷齡

封面提字：林志雄

秘書長：黃淙澤

秘書：何慈雯、許秀玲

出版單位：中華民國電腦稽核協會

展售處：中華民國電腦稽核協會

地址：11070 臺北市基隆路一段 143 號 7 樓之 4

電話：(02)2528-8875

網址：<https://www.caa.org.tw>

視覺設計：品晟股份有限公司

印刷：品晟股份有限公司

發行日期：2019 年 8 月 31 日

定價：新臺幣 250 元

著作權管理資訊

如欲利用本書全部或部分內容者，須徵求著作產權人同意或書面授權

請逕洽中華民國電腦稽核協會，電話：02-2528-8875

區塊鏈如何影響會計與審計

周濟群

美國加州州立大學蒙特利灣分校教授

自從發表了幾篇如何將區塊鏈技術應用於財務會計的文章後，本人亦有幸接受美國會計學會（American accounting association）的著名期刊 Journal of Information Systems（JIS）的邀請，擔任其 2020 年區塊鏈特刊（Blockchain technology in accounting and auditing）的客座編輯，從而也審閱了約 20 篇最新的未發表的研究，許多研究者嘗試評估區塊鏈對於會計與審計的潛在影響，雖然我在審閱論文時，對於各類型的研究題材皆保持完全客觀的立場，但相對於區塊鏈在財務會計的應用研究，於審計議題個人一直較為保守，主要原因是在尚未出現較可行的財務會計應用之前，談審計似乎有些言之過早。對於財務會計方面的應用，主要以我個人的一些研究心得為主；而至於審計方面，則由於業界許多朋友（尤其是會計師界）對於區塊鏈是否會對審計產生影響十分好奇，為了回應這些垂詢，在本文中，我也將基於目前所蒐集到的相關研究，提出一些假設性的評估，希望能激發有心的讀者們更多的想像空間，也期盼有心的國內研究者能發展出更多有趣新穎的研究議題。但由於在完稿的時點，多數參考的研究皆尚未發表，為了保護研究者的研究成果，恕筆者於本文後不附上參考文獻。

壹、區塊鏈的基本原理與概念

關於區塊鏈的基本原理與概念，簡單來說，區塊鏈就像是一種分散、公有、公開的資料儲存機制，但並非傳統安裝於某個企業或組織、能夠進行增刪修查各種交易的資料庫，它更像是眾人共同分享於網路上關於某一項資產的交易歷史。在技術上來說，在區塊鏈的 P2P 對等網路中，我們每個人（或每個節點）用自己的電腦系統來複製並共同維護、驗證區塊鏈網路上所有人的交易歷史；從使用經驗上來說，則和年輕朋友們常使用的檔案分享軟體 BitTorrent 類似：越多電腦作為種子節點在網路上分享檔案供人下載，則下載速度越快，而且檔案下載數量越多，此檔案就越難以從網路上消失。

貳、從比特幣談起

當然，對於像比特幣（Bitcoin）這種加密貨幣來說，它的目的不是數位檔案分享，而是貨幣交易歷史的分享，因此必須設定在網路上流通傳遞的最小分割單位，以比特幣為例，它的最小分割單位（Fungible unit）為 Satoshi（一個 Satoshi 是 10^{-8} bitcoin），以目前發行量

17,300,000 枚（最終發行量 21,000,000 枚）來計算，總 Satoshi 數約為 1.7315，比特幣的協定得以完整地記錄這所有 Satoshi 的交易歷史，換言之，任何比特幣自被礦工“挖出”之後，其接下來的每一個 Satoshi 所有的收付交易都會一直繼續在比特幣區塊鏈上毫不遺漏地記錄下去。因此，在以 P2P 為骨幹的區塊鏈架構上，大部份所謂的「完整節點」（Full node or full client），它們必須以複製式（Replication）的方法分散儲存所有交易歷史，而且時時和別人的那一套帳核對是否一致，簡言之，這就相當於人人手中一本帳簿，但管的不止是自己的帳，其實多數是別人的帳。

此外，在區塊鏈大量運用 Hash 技術於資料摘要（Digest）與鏈結（Link）以確保資料完整性的特殊設計之下，一個交易被正式寫入區塊鏈後，若在其後再鏈結上六個以上的區塊驗證（Confirmations），亦即區塊深度（Block depth）超過六個，則幾乎無法再以重新計算的方式重製這些經驗證的交易，因此也被視為無法再撤回或逆轉了，以目前比特幣每十分鐘產生一個區塊的速率來說，在交易寫入一個鐘頭以後，這筆交易就永遠存在比特幣區塊鏈上了，除非有人能神通廣大地把所有一半以上節點的交易資料全部取代成捏造的資料，但這對於採用了完全無法製造捷徑的工作量證明法（Proof of Work, POW）的比特幣網路共識機制而言，數學上已經證明機率是微乎其微的。

從中本聰首次提出區塊鏈的比特幣原始論文中窺探，我們或許可以說，中本聰與所有區塊鏈信徒的終極目標，是盡可能地摧毀構建於交易、管理或服務成本之上的服務模式，去除以信任為基礎的中介系

統（例如：信用卡公司），重建一個零信任（Zero-trust）、低成本、去中心化的交易模式（Nakamoto 2008）。區塊鏈如何做到呢？大致可歸因於以下兩項因素：

一、由公眾來驗證交易的存在／發生性

以往電子交易（包括信用卡、電子轉帳、電子商務等）存在／發生性的確保，必須依賴具公信力的特定第三方作為中心機構，例如：演唱會門票交易透過購票網站，電子金融轉帳透過銀行，信用卡交易透過信用卡公司，電子商務透過憑證中心（Certificate authority），證券交易透過證券交易所，房產土地交易透過地政事務所等。區塊鏈則使用所謂共識過程（Consensus progress）來取代這些中心機構的功能，以當前被視為最能達到驗證權分散目的的工作量證明 POW 為例，每個節點必須以計算力來爭取一個 Hash 數學題的解，求解這個 Hash 數學題是沒有捷徑的，只能依靠電腦以暴力法（Brutal method）不斷地試誤，雖然此法亦無法百分之百達到公平（像專業挖礦機的存在就是一例），但至少因此不像傳統指定的中心機構被永遠賦以「特權」，政府說它們大到不能倒，說漲服務費就漲，部份不肖獲授權單位還可能暗中做些圖利自己、危害社會的勾當。

以比特幣為例，所有轉帳交易被匿名記錄在公開的區塊中，且區塊間依時序連結成鏈，並經由眾人各自的電腦的閒置計算資源來驗證，因此可達到極低的交易成本（至少具有不用提供個資給中心機構、不需擔心是偽鈔、不用經過任何中介機構即可私下轉讓等好處）。換言之，眾人對區塊鏈的信任是來自於數學、來自於加密演算法，而不是來

自於對社會機制的信任，這也就是為何經濟學人雜誌在 2015 年某期的封面文章，稱呼區塊鏈為信任機器（Trust machine）的原因。經濟學人¹對區塊鏈信任的詮釋有過一個很有趣的類比，在太平洋的某個名為雅浦（Yap）的小島，島上人口只有約六千人，該島的土著人直至 20 世紀初仍在使用石幣作為流通貨幣，當地人稱這種石幣為費（Fei），在島上，越大的石幣價值越高；由於某些用於大筆支出（例如：女兒嫁妝）的石幣過於巨大而難以搬運，因此這些巨大石幣所有權的轉移，不能靠實體收付，而是靠交易雙方口頭承諾，再經由島上所有人共同確認來達成的。在某種程度上來說，這種建立在眾人確認的交易模式，和區塊鏈確實有共通之處。

換言之，區塊鏈可說是一個收錄了某項資產所有交易歷史的公共帳簿，每個區塊中包含一筆或數筆交易紀錄。如果說區塊鏈是帳簿，那麼區塊就是帳簿中的每一頁。帳簿在全網所有節點間共享，一旦有更新則會廣播通知全部節點，並立即邀請節點（在比特幣中為礦工）進行交易紀錄的驗證和更新。各節點間的關係是平等的，沒有中心伺服器節點的存在，這種分散式的架構也能在少數節點資料被破壞時，不致影響公共帳簿的完整性。而且區塊鏈連資產過去所有的交易歷史也都可以驗證，因此在交易以前，買方可以確認每項資產（如：比特幣、房地產、股票、演唱會門票等）真的為賣方所擁有，加上交易時間戳記（Time stamp）機制，更可進一步確保該資產不會同時被交易給不同買方，以免發生雙重買賣或雙重支

付（Double spending）的爭議。

二、交易事件／交易歷史皆使用公鑰加密法

當然，去中心化的成功有一些前提要件，例如：必須經過公開來讓公眾以維護整個交易，交易細節都被記錄於區塊鏈網路裡所有人皆可看到的公開帳簿上，這當然對於想要維護交易私密性的企業來說是個減分。針對此一問題，區塊鏈也有解決方案，那就是所謂的公鑰加密法（Public-key cryptography）。

在公開區塊鏈的世界中，任意兩交易雙方可以在不需公證第三方的網路環境中完成並公開他們的交易紀錄（亦即區塊），由於交易前都會經過公鑰加密法驗證雙方身份，因此交易事件是不可否認或不可逆（Non-reversible）的（交易雙方皆獲得保障）；而且藉由公鑰匿名法，技術上也可做到雖然公開了交易紀錄，但交易者是誰卻可保密，這個技術大幅增加了使用區塊鏈的誘因；當然可以預期的是，金融主管機關不會是此類匿名交易技術的粉絲，但其實因應監理需求，在技術上仍是可以採用折衷的許可式區塊鏈（Permissioned blockchain），配合實質上的 KYC 管理來避免完全匿名交易的潛在風險。

1. <http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside>

參、區塊鏈與財務會計

談到這裡，大家或許要問，區塊鏈或可稱為一種分散式帳簿，但似乎它所能記錄的僅限於單式簿記的範圍，也就是交易紀錄，而不是會計上用了數百年的複式簿記。沒錯，目前絕大多數使用區塊鏈的案例皆僅能稱得上單式簿記或會計上所稱的資產變動帳（或總帳 Ledger），要不是記錄像比特幣或以太幣這些加密貨幣的收付，要不就是登錄不動產、股票、車輛等特定資產的所有權移轉，與複式簿記上的對偶（Duality）日記帳仍有很大的差異。

因此，我的一項設計科學（Design science）研究案即利用多重區塊鏈相互勾稽、關聯的設計，來達成財會上的對偶性，當然除了建置這個假設性的多重區塊鏈平台是一項挑戰之外，另一個必須說服讀者的是經濟誘因：如何創造一個能自我支持、能持續發展的自主生態系統（Self-supporting, self-sustaining, autonomous ecosystem）？

首先我們必須思考的是，即使區塊鏈於技術上能夠支援企業的會計活動，會是什麼樣的形式？以目前市場上主要的公鏈和私鏈（或稱企業鏈、許可鏈）來說，採用公鏈的優勢是企業交易資料較易由公眾驗證其與財務報表聲明之間的關聯性（如：存在／發生、正確性、權利與義務等），但即使公鏈採用能夠匿名的公鑰技術，企業是否願意將其向來視為機密的會計資料（即使是經過）置於公鏈上則是最大的挑戰。當然，採用公鏈的另一好處是交易雙方只要使用錢包（Wallet）即可加入，不需要任何的許可，也就是說在一個支援會計紀錄的假設

性公鏈平台上，要說服你的交易對象像你一樣加入平台，並不需要花費太高的交易成本。但公鏈的驗證機制存在一個問題，由於錢包的匿名性，資產從左手換至右手，外部是很難以稽核的，因此，我們不能期待所有在公鏈上的交易都不需要再被查核，至少就可能舞弊的區域，仍必須保有專業上的注意。

至於私鏈，實則與企業內部網路類似，大部份私鏈不需要提供報酬作為誘因，也不需要太過繁複的共識演算法，只不過相對於大家較熟悉的關聯式資料庫，私鏈仍採用區塊鏈的區塊堆疊式資料結構與複製分散式儲存方法，因此在新增資料並經驗證後，也幾乎無法再更改資料內容，彈性上雖不如傳統關聯式資料庫，但在防止事後竄改上的好處卻是大大超越了傳統資料庫，再加上知名私鏈如 Hyperledger fabric 也加入 Membership service 等近乎實名許可制的 KYC 服務，私鏈在直覺上似乎是比較符合傳統會計人員的保守思維，不至於把會計資料完全曝露於公開平台上。

但運用私鏈於會計活動最大的問題是缺乏公眾驗證，即使在社群中仍可設立驗證節點，但多數是由中心機構指定的代表，因此缺乏去中心化的基本信念。另一發展障礙則是當前已存在許多成熟的會計或 ERP 系統，企業是否有必要單純為了減少外界（或會計師）對其事後竄改的風險評估而替換原本的會計系統，則是一個大大的問號。此外，私鏈或聯盟鏈必須由被授權的中心機構來審查會員資格，這也增加了企業夥伴加入成為會員的成本提高。若在企業夥伴未加入聯盟鏈的情況下，即無法有效驗證交易的存在／發生性，也就失去了使用區塊鏈對於會

計、審計最大的好處。

很明顯地，在沒有明確的解決方案出現之前，公私鏈何者較適合會計應用領域並沒有絕對的共識。因此，在我目前審閱過數篇尚未發表的研究即嘗試使用 Amazon Mechanical Turk (AMT) 服務從網路上邀集受試者進行意見調查或實驗，希望能以實證研究的角度，提供一些先期的看法。但此類研究的最大問題是研究者對於區塊鏈技術並不很熟悉，因此在實驗或問卷設計上令人產生許多效度上的疑慮，例如：由於透過 AMT 邀集的受試者通常為非專業 (Non-professional) 人士，他們必須藉由研究者提供的情境描述、問題內容等來應答或做出決策，但多數我所邀請的論文評審皆指出，大部份研究者的情境操弄或問題設計顯示他們對於區塊鏈的了解不甚正確，有的甚至會設計出明顯有利於其研究假說的情境和問題。

至於智能合約 (Smart contract) 的應用，當然也是當前會計研究者有興趣投入的一環，我的另一個研究案即嘗試使用它來合約化 (Contractualize) 複雜的會計準則，例如美國會計準則 (ASC) 第 606 號：顧客合約收入認列議題，我們試以 Solidity 在 Ethereum 上實作 ASC 606 的五步驟架構、「主理人－代理人」(Principal-Agent, PA) 以及禮品卡、顧客忠誠計畫等議題，這個研究也廣泛受到當前會計資訊研究者的重視。

肆、區塊鏈與審計

審計的根源是不信任，因為不信任公開企業會願意 (或能夠) 依 GAAP 忠實表達其財務數字，所以我們期待獨立審計服務能有

效降低這種不信任風險，從而增加資本流動的效率。然而把信任基礎放在人的身上，仍然避免不了人謀不臧的問題，近年來國內外發生的若干會計師與客戶勾結之醜聞即為明例。相對於人類，區塊鏈專家總是告訴我們，一個以數學為信任基礎、不把信任放於人類的區塊鏈網路 (A trustless blockchain network) 似乎更加值得信賴。

審計其實是一種混合了社會機制和技術的專業，一方面我們依賴複式簿記帶來的借貸方相互驗證記帳的合理性與數字正確性，另一方面我們也必須對查帳會計師的獨立性與專業道德做出規範。如前所述，在缺少明確的財會應用方向的現況下，依個人審閱論文的經驗，其實能談的不多，目前只能提醒審計人員，在未來越來越多企業使用區塊鏈來記帳的前提下，查核的第一要務是要蒐集查核客戶的錢包資料，因為裡面存放了客戶在區塊鏈上的交易資料。當然，若你是聯盟鏈的支持者，可能會想到是否能將會計師列為交易驗證節點，指定他們驗證客戶的交易，並且將審計要求的查核目標置入該鏈的驗證協定之中，亦即 Confirmation 等於 Audit，這當然不是不可能發生的，但這樣的情境和目前的審計實務並無太大的差別，企業是否願意由現行實務轉為加入聯盟區塊鏈？對他們有何好處？目前看來，這個概念的落實仍需要主管機關的強制規範。除非美國證管會 (SEC) 被說服這麼做能大幅提升審計品質與效率，否則不容易由民間發動。

此外，適當的財會區塊鏈上的交易資料，基於其無法篡改 (Tamper free) 的特性，理想上可作為查核人員所需要的原始憑證，當然這仍需要查核人員依前述建議，先

蒐集客戶錢包以核實其有無左手賣右手的情況，換言之，Tamper free 不等於 Fraud proof，無論區塊鏈如何發展都無法完全解決人謀不臧的問題，筆者建議千萬不可掉入支持者過度樂觀的話術中。

伍、小結

在看過本篇之前，讀者們可能也曾聽說區塊鏈是一種分散式帳簿（Distributed ledger）或者「超帳本」（Hyperledger），或許你內心想著：「什麼？這跟會計、審計有什麼關係？」的確，當其它領域的專家在借用會計領域術語時，有時會誤用，或使用時有點令行內人感到混亂，但這次可並沒有用錯。對於實務從事會計、審計業務的人士來說，首要之急是評估此一技術將如何影響我們未來的會計審計工作；而對於學術研究者而言，則應更加深入研究此一技術，並嘗試創造出新的會計、審計架構。因此，本文一開始先簡介若干區塊鏈的基本技術概念，以此作為評估區塊鏈影響的基礎，再來依筆者個人研究、審閱經驗，從會計審計專業的角度來詮釋這些技術概念，同時提出一些當前思想新穎的前期研究者的「奇思異想」供大家發想。

自抹除、刪除與抹除權及被遺忘權之控制措施的標準化談「設計及預設的資料防護」：根基於雲端運算服務

A discussion in “Data protection by design and by default” start from the controls standardization of “erase”, “delete” and “right to erasure” (‘right to be forgotten’), based on cloud computing service

蔡昀臻

臺灣網路防護協會

yct1230@gmail.com

樊國楨

臺灣經濟新報文化事業股份有限公司

kjf.nctu@gmail.com

摘 要

2016年4月14日經歐洲議會通過、4月27日公布之「一般資料保護規則(General Data Protection Regulation, GDPR)」,提出個人資料「擬匿名化」之新定義並於條款17提出「抹除權(『被遺忘權』), Right to erasure (‘right to be forgotten’)」。本文就該條款之「抹除(Erase)」敘明其技術議題以及比較美國與中國大陸的標準化進程;

進而，提出我國宜增設之抹除權（「被遺忘權」）的規範。

2014 年歐盟法院在 Google v. AEPD 案的判決中針對該議題提出其法律觀點，確認「被遺忘權（Right to be forgotten）」為歐盟公民擁有的權利。GDPR 條款 17 規範「資料控制者」，除執行前述的「資料主體」之要求「抹除個人資料」（第 17 條第 1 項）外，尚需通知其他第三方「抹除個人資料」（第 17 條第 2 項）。

美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）從資料清理觀點定義，「刪除（Delete）」一筆資料僅需於存取檔案時已無前述的資料即可，通常作法僅將連結此筆資料的指標移除；換言之，此筆資料的物理紀錄尚存在於儲存媒體之中。「抹除」則是等同於「應用最先進之實驗室的物理性技術（例：消磁）的邏輯性技術，以確保目標資訊無法被恢復；隨著 GDPR 之實施，「抹除」的實作將日益普及，ISO/IEC CD 27552.2 已將其納入控制措施中。

2017 年 5 月 29 日，中國大陸公布之《信息技術個人信息安全規範》，第 3.9 節修訂「刪除：在日常業務場景和操作所涉及的系統中去除個人信息，使其不可被檢索、訪問、傳輸且不能復原的行為」，惟「抹除物理痕跡」於現階段之互聯網企業尚無法達成；應然與實然調和後，同年 11 月 30 日再修訂「刪除」之定義為「在實現日常業務功能所涉及的系統中去除個人信息的行為，使其保持不可被檢索、訪問的狀態」，並於 2018 年 5 月 1 日正式實施。中國大陸 PIMS 之「刪除」的「術語和定義」之標準化的過程，宜借鏡之。

「他山之石，可以攻錯」，多年來，我國 ISMS（Information Security Management System）與 PIMS 的實作卻以通過驗證為標的，致使事倍功半，前述中國大陸誤將「刪除」之規範作為「抹除」的驗證標準即為例證！歐盟與美國的經由規範以及評鑑與測試 ISMS 及 PIMS「行為準則」之遵循，及其經由法規制約 ISMS 與 PIMS 的控制措施之標準化，是值得我們深入研究的議題；本文以「抹除」為例，探討其應為。

關鍵詞：抹除、刪除、抹除權、被遺忘權、一般資料保護規範

Abstract

On April 14, 2016, General Data Protection Regulation was adopted by the Council of the European Union. GDPR redefined pseudonymised data and propose “right to erasure (‘right to be forgotten’)” in article 17. Thus, we focus on “erase” technique mentioned in the article and compare the standardization processes between America and China in this article. Furthermore, we propose that the government should add the idea “Right to erasure (‘right to be forgotten’)” into our standard.

In the arguments of Google v. AEPD in 2014, the European court of Justice offer its view point that “Right to erasure (‘right to be forgotten’)” is an EU citizens’ right. In GDPR article 17 states that once being asked to erasure, the controller shall not only erasure the data, but also take reasonable steps to inform other controllers which are processing data that data subject has requested the erasure.

National Institute of Standards and Technology defines “delete” as couldn’ t find data when accessing from the data sanitization point of view. The usual way of doing so is to remove the pointer pointed to the data. In other words, the data is still stored in the media. On the other hand, “erase” is equal to apply physical or logical techniques that render target data recovery infeasible using the states of the art laboratory techniques. With the implementations of GDPR, the “erase” implements also become universal. ISO/IEC CD 27552. 2 has already included it into its controls.

On May 29, 2017, China released “Information Technology – Personal Information Security Specification” . In section 3.9 revision states “Delete: The act of removing personal information from the systems, involved in daily business scenarios and operations, so that it cannot be retrieved, accessed, transmitted, and cannot be recovered.” . However, internet companies could not achieve “erase physical trace” requirement for now. As a result, the definition of “delete” was revised as “the act of removing personal information in the systems, involved in the daily business, so that it remains unable to be retrieved and accessed” and come into effect on May 1, 2018. The process of China’ s Personal Information Management System (PIMS) standardization on terms and definitions of “delete” should be viewed as an example.

For many years, we have only set goals of Information Security Management System (ISMS) and PIMS implements on passing verifications and thus the effect is limited. The misuse of the “delete” specification as the “erase” verifications mentioned above is an example. The EU and the USA follow the specifications and the assessments and tests of ISMS and PIMS “code of conduct” . Their regulations on ISMS and PIMS standardization controls worth our further study. Thus, we take “erasure” as an example and discuss what should be done.

Keywords: Erase, Delete, Right to erasure, Right to be forgotten, General Data Protection Regulation (GDPR)

壹、前言

2012年1月，歐盟開始整合「個人資料保護指令 (Directive 95/46/EC)」、「電子通訊隱私指令 (Directive 2002/58/EC)」與「電信網路改革指令 (Directive 2009/136/EC)」三大個人資料及隱私防護指令之法制，期以單一規則 (Regulation) 簡化機關/構以及企業的法規遵循義務並促進單一數位市場；2016年4月14日經歐洲議會通過，於2016年4月27日公布之「一般資料保護規則 (GDPR)」，已提出個人資料「擬匿名化」之新定義並於條款11闡明「去識別化」的應然，第17條款提出「抹除權」(「被遺忘權」) (Right to erase) (‘Right to be forgotten’)，條款25闡明應根基於「從設計以及預設機制著手保護個人資料 (Data protection by design and by default)」實作個人資料管理系統 (Personal/Privacy Information Management System, PIMS) 之合適的「技術控制措施 (Technical measures)」與「組織控制措施 (Organizational measures)」(Official Journal of the European Union 2016)。GDPR 於第40~43條款規範其「行為準則及驗證 (Codes of conduct and certification)」，認證機構遵循產品驗證標準規範驗證機構；根基於GDPR，相關機構幾均公布採用ISO/IEC 27001作為其包含資料去識別化的PIMS合規之驗證要求事項的規範 (Official Journal of the European Union 2016)。

2017年1月，依據GDPR第42條款，European Privacy Seal (EuroPrise) 公布GDPR驗證之共同準則，闡明於「資訊技術服務」將採用ISO/IEC 27001與ISO/IEC 27009 (未來為ISO/IEC 27552) 作為驗證標

準「產品 (含「軟體作為服務 (Software as a Services, SaaS)」等資訊系統)」採用ISO/IEC 15408標準系列 (Common Criteria 2019; ISO 2018g) 作為驗證標準，以為GDPR條文中「組織控制」以及「技術控制」稽核的頂層設計原則，並於2017年1月公布其自2007年8月起準備之GDPR驗證準則，德國、英國、西班牙等試運行中 (EuroPrise 2017; ISO 2017)；GDPR第41條款規範PIMS之主責人員的「行為準則 (Codes of conduct)」，第43條款規範ISO/IEC 17065之「產品、過程與服務驗證機構認證規範」為認證機構稽核驗證機構的標準；並於第51~59條款，闡明其目的事業主管之「獨立監督機構 (Independent supervisory authorities)」的權責。本文僅就其第17條款中之「抹除」，敘明其技術議題以及比較美國與中國大陸的標準化進程，取徑於此，以闡明我國宜增設抹除權 (被遺忘權) 實作規範之應然。

2014年5月13日，歐盟法院宣布“Google Spain SL, Google Inc. v. AEPD”之最終判決的理由：「對於在原為合法處理之正確資料，因時間的推移，或因當初被蒐集及處理之目的已不再為必需，致使已不合法規 (歐盟 Directive 95/46/EC (個人資料保護指令)) 之意旨，尤其是鑑於原目的因時間之流逝而成為「不適當、不相關或不再相關、或過當 (Inadequate, irrelevant or no longer relevant, or excessive)」的情境。……資料主體得基於前述法規第12條第b款提出要求，……搜尋結果中之相關資訊及其連結即應被移除。」成為「被遺忘權」的源池；此外，歐盟法院限縮資料主體僅能就網

際網路上可以經由搜尋引擎搜索到的、對資料主體之不適當、不相關或不再相關、或過當的個人資料行使「被遺忘權」，並負舉證責任。根基於前述法理，Google 有義務抹除 1998 年 Mario Costeja Gonzale 關於其償付社會安全債務之不動產拍賣公告的資訊；成為「被遺忘權」之具體適用規則（紀珮宜 2017）。GDPR 條款 17 規範「資料控制者」，除執行前述的「資料主體」之要求「抹除個人資料」工作項目（第 17 條款第 1 項）外，尚需通知其他第三方「抹除個人資料」（第 17 條款第 2 項）（Official Journal of the European Union, 2016）。

根基於 GDPR 及 PIMS 標準化之歷程，本文在第 2 節闡明「抹除」標準化之進程；於第 3 節，探討雲端運算與「抹除」等 PIMS 要求事項的新議題及其已納入 ISO/IEC CD 27552.2 之擴增 ISO/IEC 27001 的 PIMS 驗證之「抹除」要求事項進程的闡明；最後，在第 4 節提出借鏡個人資料管理系統標準化之「從設計著手及以預設機制防護隱私 (Privacy protection by design and by default, PbD)」進程與議題，作為我國 PIMS 及抹除資料標準化藍圖參考的見解並代為本文之結論。

貳、刪除與抹除

2017 年 1 月，依據 GDPR 第 42 條款，EURO Privacy Seal(EuroPriSe) 公布之驗證準則 (Criteria)，其內容分成「基礎議題概觀 (Overview on fundamental issues)」、「資料處理之合法性 (Legitimacy of data Processing)」、「技術 - 組織控制措施 (Technical-organisational measures)」與「資料

主體權利 (Data subjects rights)」4 部分，「抹除權」係屬「資料主體權利」，PbD 為「基礎議題概觀」之基石；換言之，抹除的實作於 PIMS 組織控制係確保符合法規要求事項之合理運作，其技術控制宜納入 PbD 以確保「抹除」運作過程資訊技術的到位；在此，先敘明其與「刪除」之差異。資訊系統中之「刪除」一筆資料僅需於存取檔案時已無前述的資料即可，通常之作法僅將連結此筆資料的指標移除；換言之，此筆資料的物理紀錄尚存在於儲存媒體之中，於敏感性或機密性資料宜執行如圖 1 所示的「資料清理 (Data sanitization)」作業。「刪除」宛如檔案室雖已禁止調閱一指定文號之公文，惟其公文實體仍存放於檔案櫃中，自然無法完全阻絕有心人存取此公文的機會；於雲端服務之核心符合性要求事項之第 10.12.7.3 節的「資料刪除過程」即要求：「資料刪除過程之定性目的 (cloud Service Qualitative Objective, SQO) 應將雲端服務提供者 (Cloud Service Provider, CSP) 致使不能回復 (Irretrievable) 已刪除資料之過程文件化。」(ISO 2017)。「抹除」則係屬資料清理作業中，應用物理 (Physical) 或邏輯 (Logical) 之技術，確保標的資訊無法在實驗室之「發展中的科技之目前頂級能力 (State of the art)」中，致使其資料被「回復」的「廢止」中之「抹除」的邏輯技術 (Kissel, R. et al., 2014)，其物理技術為「消磁」；換言之，「刪除」不完全符合前述歐盟法院 2014 年 5 月 13 日的「被遺忘權」最終判決之意旨，GDPR 敘明其為「抹除權」，以括號闡明等同於「被遺忘權」。GDPR 的「抹除權」(「被遺忘權」)之「實作 (控制措施)」的「技術控制」係指圖 1 中「廢止」之邏輯技術中

的「區塊抹除」或「密碼式抹除」(Kissel, R. et al., 2014)；2013年起，CPU 均內嵌能執行抹除功能的組件，且已建立檢測機制，隨著 GDPR 之實施，「抹除」的實作將日益普

及，ISO/IEC CD 27552.2 已將其納入控制措施中，如表 1 所示 (ISO 2014; ISO 2016; ISO 2018a)。

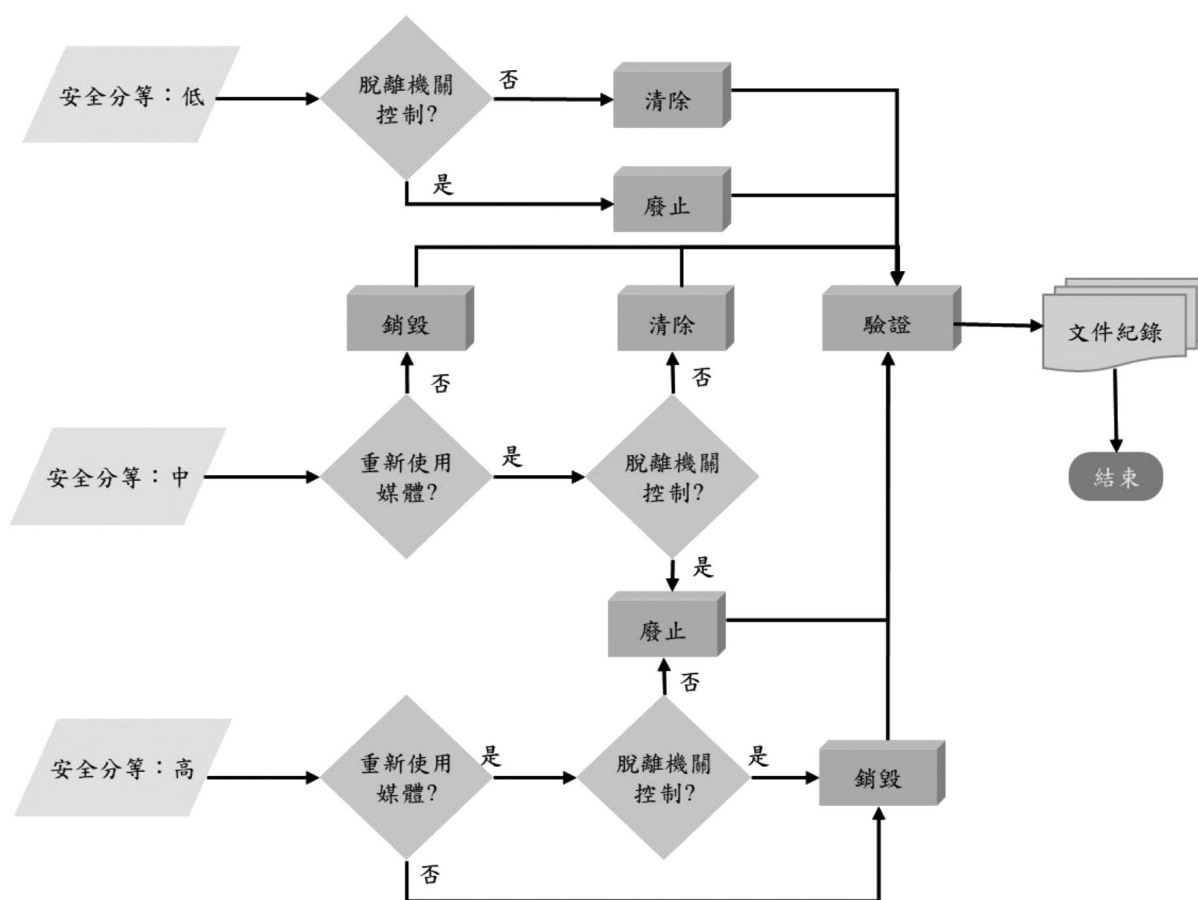


圖 1 資料清理 (Sanitization) 與處理 (Disposition) 決策流程 (Kissel, R. et al., 2014)

說明：

1. 清除 (Clear)：使用邏輯性技術 (Logical techniques) 來清理 (Sanitize) 所有用戶可定位 (User-addressable) 之儲存位置的數據，以防止簡單的非侵入式 (Non-invasive) 資料恢復技術。
2. 廢止 (Purge)：使用最先進之實驗室的物理性輯性技術，使目標資料無法恢復。
3. 銷毀 (Destroy)：使用最先進的實驗室技術使目標資料無法恢復且使得後續無法使用該媒介 (Media) 儲存資料。

表 1 ISO / IEC 27552 之組織證據 (Organizes evidence) 與標準 (本研究製作)

技術與組織之控制措施 (Technical & organizational measures)	<ul style="list-style-type: none"> 去識別化(De-identification)(ISO/IEC 20889)與抹除(Erasure)(ISO/IEC 27040)以支持資料最小化(Data minimization) 接收(Receiving)、記錄(Documenting)和修改(Modifying)同意書 支援資料主體之權利(存取(Access)、可攜帶(Portability)、修正(Correct)及抹除) 資訊安全遵照 ISO/IEC 27001、ISO/IEC 27002 以及 ISO/IEC 29151
記錄保存 (Record keeping)	<ul style="list-style-type: none"> 處理之目的 處理之合法基礎 對第三方單位之揭露(Disclosure)與傳送 地理位置(Geolocation) 為了負責(Accountability)而保存紀錄
規範遵守之展示 (Demonstrate adherence)	<ul style="list-style-type: none"> 處理者之義務遵照 ISO/IEC 27018 資料主體之風險遵照隱私影響評鑑(Privacy impact assessment)，即 ISO/IEC 29134，從設計著手及以預設機制進行保護資料(Data protection by design and by default, PbD)(ISO/IEC 29101 以及 ISO/IEC 27550) 同意與告知(ISO/IEC 29184)、資料可攜性(ISO/IEC 19941)、自動決策以及剖析(Profiling)(待定)
資料主體的透明性 (Transparency to data subjects)	<ul style="list-style-type: none"> 資料主體之透明性遵照 ISO/IEC 19944 之資料使用之陳述 控制者、處理者之透明性遵照 ISO/IEC 19086

使用密碼學技術之「密碼式抹除 (Cryptographic erase)」亦可執行「清除」與邏輯性技術「廢止」的工作項目，並提供「金鑰回復 (Key recovery)」之選項，提供系統停機時自動保護資料的控制措施 (ISO 2016)；以磁碟機為例，具備前述之整合「存取控制 (Access control)」的「密碼式抹除」之整體功能者名為「自加密磁碟機 (Self-Encrypting Drives, SED)」(Kissel, R. et al., 2014)，於「雲端運算服務水準協議」標準系列的 ISO/IEC 19086-1:2016(E) 中之第 10.12.8.1 條款敘明可以圖 1 的「資料清理」過程代替「資料刪除 (Data deletion)」；換言之，於實作，SED 已是雲端服務供應者 (Cloud Service Provider, CSP)「資料刪除組件 (Data deletion component)」的元件之一 (ISO 2016)；鑑於諸如離線磁碟機、暫存檔安全控制的攸關性，圖 2 所

示之「雲端運算服務」標準化的示意說明 (ITU 2016)，已將圖 1 以及如圖 3 所示的 SED 等「事實標準 (De facto standard)」擴增制定 ISO/IEC 27040(ISO 2015; Willett, M 2009)，並將「抹除」納入 ISO/IEC 27018 之控制措施中 (ISO 2014)；於 PIMS 要求事項的 ISO/IEC CD 27552.2 之第 A.7.3.7 節闡明「組織宜實作向個人可識別資訊 (Personally Identifiable Information, PII) 當事人 (Principal) 履行存取、更正及 / 或抹除其 PII 義務之政策、程序及 / 或機制 (ISO 2018a)；於 EuroPriSe 的驗證準則，在「抹除」的稽核要求除「組織控制措施」外並闡明其執行方法應判斷其是否為「不可逆 (Irreversible)」，若抹除資料係使用「覆寫 (Overwriting)」則須判斷其次數是否足夠等根基於 PbD 之「技術控制措施」工作項目 (EriPriSe 2017; ISO 2015a)。

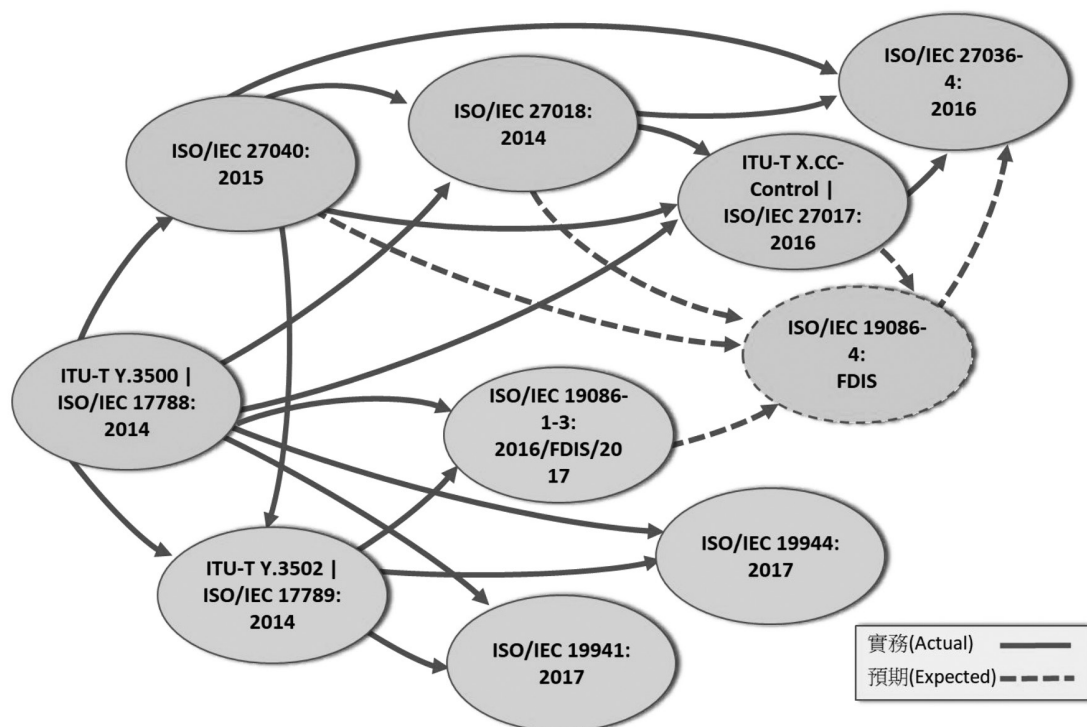


圖 2 雲端運算標準化路徑圖（本研究製作）

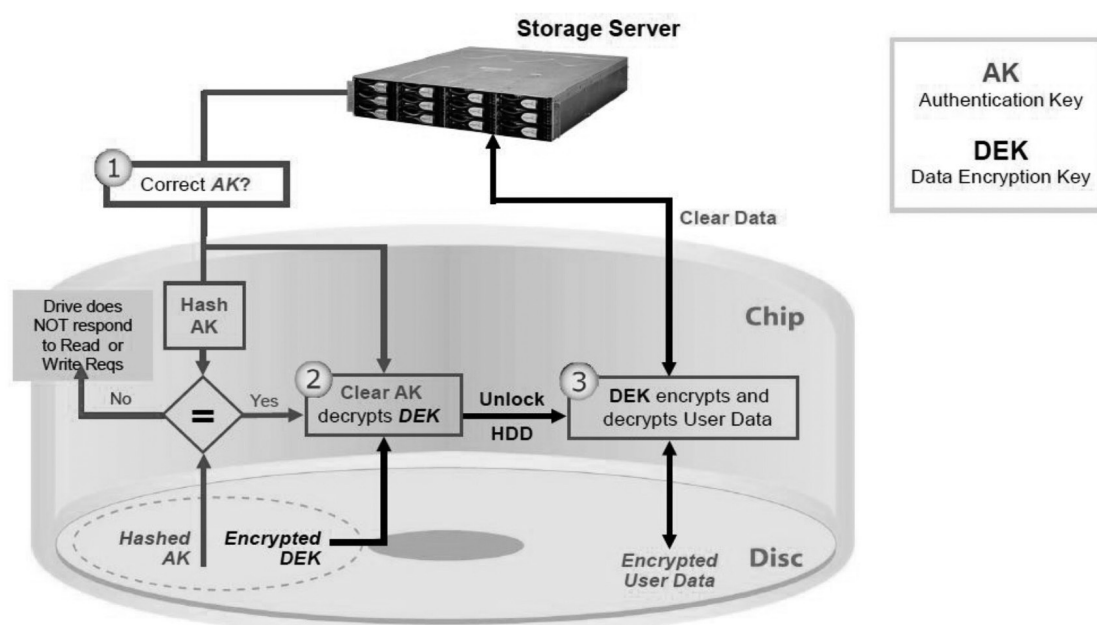


圖 3 磁碟機 SED (Self-Encrypting Drives) (Willett, M., 2009)

於美國，健康、金融等領域，如表 2 所示，均以法規要求執行「資料清理」工作項目以保護個人資料，並制定 US\$ 10,000~1,000,000 與「1% 之資產 (1% of assets)」等的未執行「資料清理」之相關罰

則 (Hughes, Gordon, and Tom Coughlin 2006)，「抹除」亦已成為資訊安全課程內容的項目 (ACM, IEEE-CS, AIS SIGSEC and IFIP WG 11.8 2017)。

表 2 要求執行資料清理之美國相關法規列表（本研究製作）

法規名稱
健康保險可攜與責任法 (Health Information Portability and Accountability Act, HIPAA)
個人資訊保護與電子文件法 (Personal Information Protection and Electronic Documents Act, PIPEDA)
格雷姆 - 里奇 - 比利雷法案 (Gramm-Leach-Bliley Act, GLBA)，亦稱金融服務現代化法案 (Financial services modernization act)
加州資料隱私法案 (California senate bill 1386)
沙賓法案 (Sarbanes-oxley Act, SBA)
美國證券交易委員會 (United States Securities and Exchange Commission, SEC) 規定：第 17a 條 (SEC Rule 17a)

綜前所述，雲端運算旨在提供使用資訊像油水電等關鍵基礎設施一樣成為數位社會之基礎建設，惟面向服務的資料運算在運作面向必然是資源共享，如何解決資源共享引發之資訊安全疑慮已是雲端運算是否可信賴的攸關性之議題；已成為事實標準的使用可信賴計算平台 (Trusted Computing Platform, TCP) 之可信賴執行技術 (Trusted Execution Technology, TXT) 的開放證言 (Open Attestation, OAT) 與開放雲完整性技術 (Open Cloud Integrity Technology, Open CIT) 均植基於 TCP 之可信賴平臺模組 (Trusted Platform Module, TPM)，有效防護惡意程式碼之 TPC 是一個富於創造性的研究與發展領域，歷經從保密到防護，更進而整合密碼模組及安全作業系統 (Secure Operating System, SOS) 提出並實作之，圖 4 是其框架示意說明 (ISO 2014；ISO 2015a；ISO 2015b；ISO 2016；ISO 2017；ISO 2018a；Brito 2017；Yeluri and Castro-leon 2014)，TPM 是圖 3「磁碟機 SED」之關鍵組件 (Common Criteria 2018；

Intel 2017；Trusted Computing Group 2018)。

1999 年 10 月，AMD、HP、IBM、Intel、Microsoft、SONY、SUN 共同發起成立可信計算平台聯盟 (Trusted Computing Platform Alliance, TCPA)，3 年間，發展成員約 200 家，遍布全球各國主要廠商；根基於 TCPA，2003 年 4 月 8 日，70 個資訊技術 (Information Technology, IT) 公司根基於：「使用增加之硬體組件，增進安全」與「資料之最終防護僅由加密功能提供」的假設，成立了可信賴計算集團 (Trusted Computing Group, TCG)，2003 年 5 月，TCG 公布 TPM 1.0 規範，TPM 1.2 增加了其對字典攻擊法的防護；2004 年，密碼學家提出攸關 TPM 1.2 安全之 SHA-1 的重大攻擊方法，此攻擊方法雖然並不適用於 TPM 中之 SHA-1 的使用方式，惟密碼演算法隨著時間之推移只會愈來愈不安全是密碼學的共識；2005 年，TCG 開始制定 TPM 2.0 的規範，TPM 2.0 於密碼使用識別符，從而可以在不改變 TPM 標準之狀況下使用任

何密碼演算法，此外亦增進其安全及管理的可用性；2014年，TPM 2.0 正式使用，2015 成為 ISO/IEC 11889 系列標準 (ISO 2015a;

ISO 2015c) 並已建立產品驗證機制 (Common Criteria 2019)。

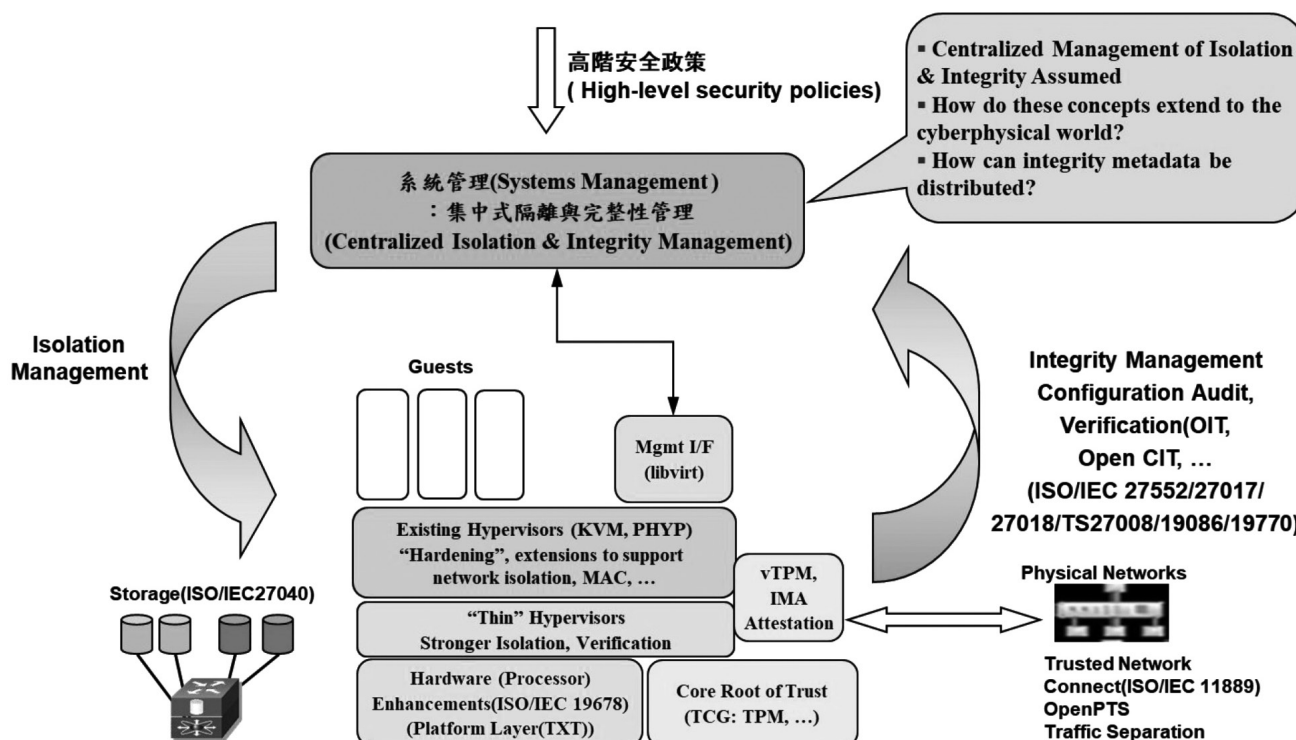


圖 4 雲端運算之細緻 (Fine-grained) 的資訊安全部署：隔離 (Isolation) 與完整性 (Integrity) 之封閉循環 (Closing the loop) 框架 (備考：此框架係 IBM 於 2011 提出)。

參考資料：<http://www.apress.com/br/book/9781430261542/> (last visited 2018-12-07)

目前「行政院國家發展委員會」之「歐盟個人資料保護規則專區」於 GDPR 的中譯，將「刪除」與「抹除」均譯為「刪除」，宜闡明之 (Hughes, Gordon, and Tom Coughlin 2006)，並兼及其組織控制與技術控制，以及執行「抹除」功能的組件宜有之測試及評估 (Kissel, R. et al., 2014; ISO 2018b)。中國大陸先於 2017 年 5 月 29 日公布「GB/T 35273(報批稿)：信息技術 個人信息安全規範」中第 3.9 節「刪除：在日常業務場景和操作所涉及的系統中去除個人信息，使

其不可被檢索、訪問、傳輸且不能復原的行為」，惟「抹除物理痕跡」於現階段之互聯網企業尚無法達成；應然與實然調和後，2017 年 11 月 30 日修訂其「刪除」之定義為「在實現日常業務功能所涉及的系統中去除個人信息的行為，使其保持不可被檢索、訪問的狀態」，2018 年 5 月 1 日 GB/T 35237 正式實施 (中國國家標準化管理委員會 2017)，惟其實作之標準化尚在進行中。中國大陸 PIMS 的「刪除」之「術語和定義」的標準化過程，宜借鏡之。

參、抹除與個人資料管理系統要求系統之PbD控制措施初探

九十年代全球文明歷經了重大的轉變，品質、環境和職業安全衛生管理逐漸朝向一致化與標準化，而相關的國際標準也影響了許多國家經濟的發展以及組織管理與經營的方式，ISO 9000 品質管理和 ISO 14000 環境管理系列標準的遵循，就是最佳的佐證。

「讓過去與現在爭執不下，將錯失未來 (Opportunities for future will be missed if the past is allowed to argue with today)」，ISO/IEC JTC 1/SC 27 主席 Walter Fumy 先生在世界資訊高峰會之邀請下，於 2004 年 9 月 24 日公布了 ISO 之深度防禦 (Defense in depth) 的資訊安全管理模型觀點；其標準組件 ISO 27001 標準系列之 ISO/IEC 27003 已於 2010 年 2 月 1 日正式發行，ISMS 標準化的第一階段工作已樹立第 1 座里程碑。

鑑於管理系統日益增多，其標準系列宜加以規範，國際標準組織 (International Standardization for Organization, ISO) 自 2000 年起即分 3 階段進行管理系統標準 (Management System Standards, MSS) 之標準化工作；已正式納入 ISO 之強制性規範 (Procedures specific to ISO)，期能在第 3 階段 (2011~2015 年) 完成各個管理系統要求事項的調和。ISO/IEC 27001 標準系列已遵循 MSS 逐步建立中，並納入個人資料/隱私管理系統 (Personal/Privacy Information System, PIMS) 安全規範之議題；以個人資料保護法施行細則第 17 條之規範為例，已公布 ISO/IEC 27009、ISO/IEC 29101、ISO/IEC 29191、ISO/IEC 20008 與 ISO/IEC 20009 標準系列，作為其 PIMS 中「前臺匿名、後臺

實名」之實作要求事項的參考。2012 年 10 月，ISO/IEC JTC 1/SC 27 在進行為期 1 年之 2 階段的研究後，正式公布 PIMS 之要求事項遵循 ISO/IEC 27001，同時開展其標準系列 (ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 27017、ISO/IEC 29134、ISO/IEC 29101、ISO/IEC 29151 以及預備文件 SD 4、SD 5 等) 的標準化計畫，已於 2017 年 8 月完成第 1 階段之工作項目；並根基於歐盟與美國聯邦政府實作意見分成「管理」、「實作」與「技術」3 個面向，進行第 2 階段的標準制訂之計畫。

研究「標準化」的人是需要有「同情」與「推理」兩種能力，所謂「同情」是指「標準」的制定者要有對等之情，那樣體驗的「標準」自然是立體、多元的；「同情」加上「推理」，則「標準」是活的，每一份「標準」的頒布是因或是果，是趨勢或是成績，「標準」的產生絕非偶而是無數之努力的形成。「標準化」從長遠的角度來看，便可以體察出是有一股流勢，有無法阻擋的推移力量；MSS 與個人資料保護標準化及 ISMS&PIMS 的整合性 (資訊) 安全管理系統 (Integrated (Information) Security Management System, IISMS) 之進程僅為一端。國際認證論壇 (International Accreditation Forum, IAF) 自 2013 年 3 月 25 日起，已發行整合性 (資訊) 安全管理系統 (IISMS) 之第三方稽核的強制性文件 (IAF MD 11: 2013)，除規範 ISMS 之第三方稽核的要求事項外並闡明其效益。根基於 IISMS 與雲端服務已成為資訊社會之基石，主責 ISMS&PIMS 標準化的 ISO/IEC JTC 1/SC 27 第一階段標準化之工作項目如圖 5 所示 (ITU 2016)，已於 2017 年完成，其中「PII 原則

係指國際公認之隱私原則」；惟於技術控制實作闡明的需求，2019-01 公布的 ISO/IEC TS 27008 已擴 / 新增圖 5 中之 ISO/IEC

27018、ISO/IEC 27017 及 ISO/IEC 29511 的控制措施列於其附錄 C 之中 (ISO 2019a)。

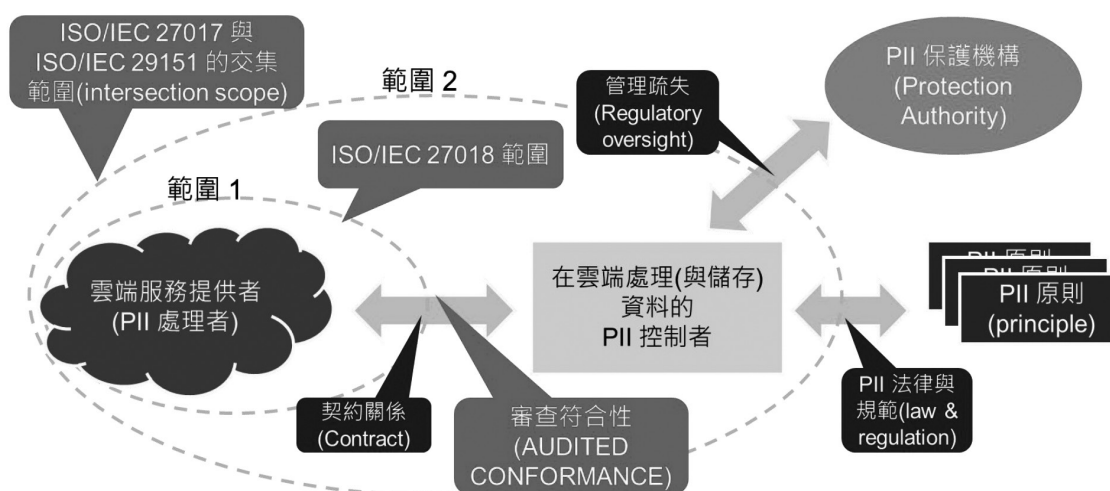


圖 5 雲端運算之 PIMS 控制措施的框架

說明：

1. PII 控制者 (PII controller) (或稱為資料控制者於某些管轄區 (jurisdiction)) 意指決定個人資料處理或將要處理之目的與方法之當事人 (單獨一人、與他人共同)。
2. PII 處理者 (PII processor) (或稱為資料處理者於某些管轄區) 意指代表 PII 控制者處理資料之任何人 (除了 PII 控制者的僱員外)。
3. 資料來源：Mitchell, C. (ISO/IEC 27018 編輯), Outsourcing personal data processing to the cloud (presentation), 2012-02-16，圖中之「交集範圍 (intersection scope)」係指「聚集」。

於歐盟與美國，PIMS 實作「抹除」已多年，ISO/IEC CD 27552.2 在第 7.3.7 條款規範之；「共識是標準化的源池，實作係標準化之基石」，若同前述中國此議題「應然與實然」的考量，ISO/IEC 27018 擴增之第 A.10.13 控制措施的實作指引中敘明：「……，效能議題可能意謂明確抹除該等資料是不切實際的。如此產生另一使用者可能可以讀取該資料之風險。宜藉由特定技

術的控制措施以避免該風險。……，舉例而言，某些雲端架構下，若雲端服務使用者嘗試讀取未被該使用者本身資料覆蓋的儲存空間，平臺或應用系統將回傳一串 0。」(ISO 2014; ISO 2018a)，離線後再執行應有之抹除；參照 PIMS 控制措施標準化的發展之進程 (ABAC 2019; Grass 2018; ISO 2018f; Rannenberg 2017)，圖 6 為 ISO/IEC JTC 1/SC 27 在 2017 年 1 月公布的 PIMS 標準化

框架 (ISO 2018f), 「抹除」已納入 ISO/IEC CD 27552.2 之控制措施中 (ISO 2018a), 圖 4 的實作宜遵照 GDPR 之 PbD 的要求事項; 綜前所述及「抹除」實作之 ISO/IEC 11889 系列標準的技術性, 其「組織之控制措施」應以 PbD 的「技術控制」支持之

(ENISA 2014; ISO 2013; ISO 2018c)。前述 ISO/IEC CD 27552.2 於 2019-06-25 進入國際標準 (International Standard, IS) 的發行 (Publication) 階段, 2019-07 改號為 ISO/IEC 27701, 2019-08 出版 (Published) (ISO 2019b)。

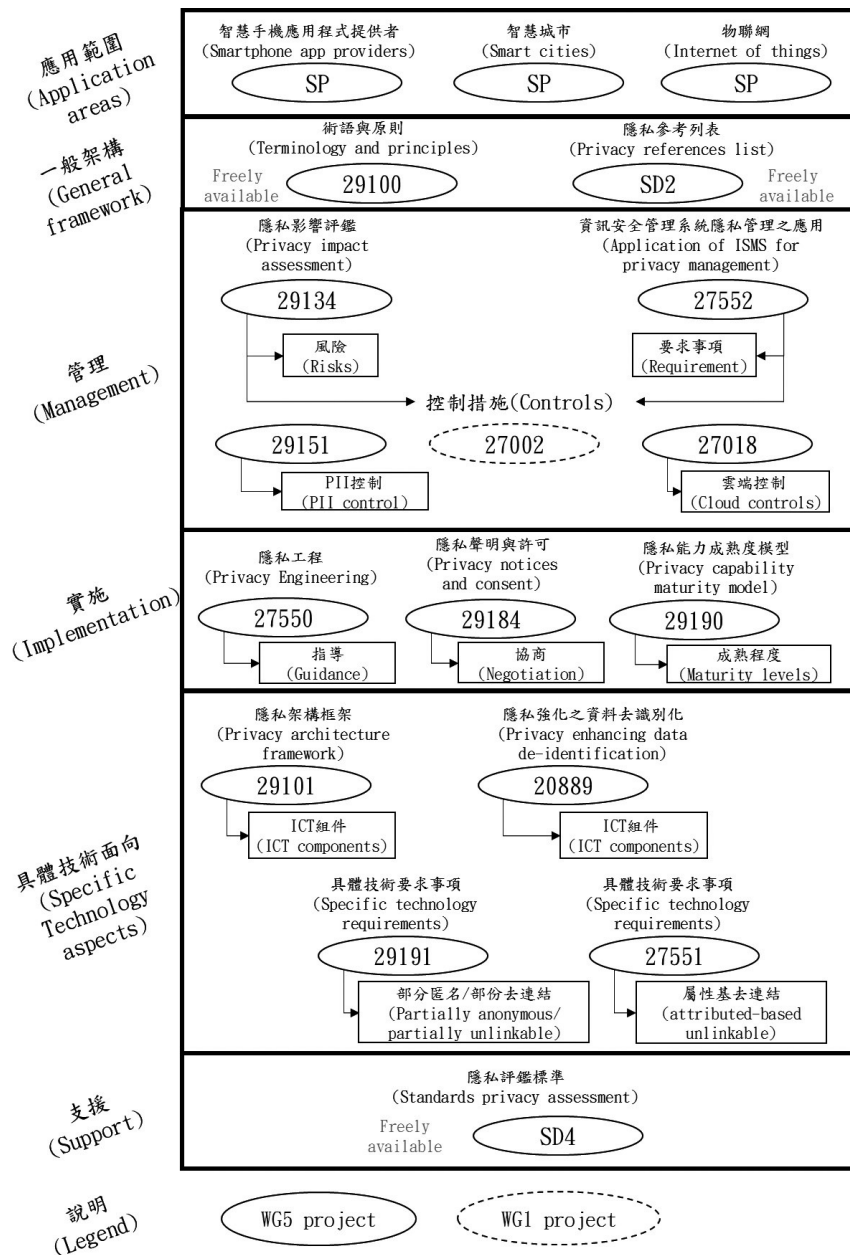


圖 6 個人資料管理要求事項之 ISO/IEC JTC 1/SC 27/WG 5 與 WG 1 的標準化框架 (ISO, 2018f)。

說明: ISO/IEC 27551 及「智慧手機應用程式提供者」2 項議題, 為本文作者自行加入此框架。

GDPR 第 25 條款之「設計及預設的資料保護 (Data protection by design and by default)」之要求事項即為 PIMS 通稱為 PbD 的「從設計著手及以預設機制防護隱私」，「抹除」於 PIMS 控制措施之實作宜屬 PbD 應為的工作項目之一，PbD 是「考量到現有技術、執行成本以及處理之性質、範圍、內容與目的以及處理對當事人之權利及自由所生諸多可能且嚴重之風險，不問係在決定處理方式時或係在處理中控管者均應實施適當的技術及組織的控制措施，例如「擬匿名化 (Pseudonymisation)」，且該等控制措施旨在實現資料保護原則，如資料最小蒐集原則，並採取有效方式將必要防護措施 (Safeguards) 納入處理程序，已符合 GDPR 之要求事項並保護資料主體的權利。」、「控管者應實作適當之技術及組織控制措施，以確保在預設情況下，僅處理一特定目的且於必要限度範圍內之個人資料，該義務適用於所蒐集的個人資料之數量、處理之程度、儲存的程度、儲存之時間與其可接近使用性。尤其是該等控制措施於預設情況下，應確保個人資料不能經由人為干預而遭不特定人之接近使用。」是規範 PbD 的 GDPR 第 25 條第 1 項及第 2 項所定之要求事項 (Official Journal of the European Union 2016)；根基於此，圖 4 實作的技術及組織控制，除表 3 之組織控制措施外，ISO/IEC CD 27552.2 第 6.11.2.5 節要求的如表 4~表 7 之隱私工程亦應納入 (ISO 2018a; ISO 2018c)，EuroPriSe 於 PbD 的稽核要求除組織控制措施外，並闡明應判斷其資料「去識別化」係自動化或根據要求處理與資料之重新識別風險等技術控制措施 (Chatila 2019; EuroPriSe 2017; ISO 2018d)。

於 ISO/IEC 27002 的「系統獲取、開發與維護」控制措施之實作指引中規範遵循「軟體工程」與「隱私架構框架」(ISO 2018a; ISO 2013)，於 PIMS 之控制措施的實作除機密性、完整性與可用性外尚需考量「分離性 (Disassociability)」、「可調解性 (Intervenability)」、「可管理性 (Manageability)」、「可預測性 (Predictability)」、「透明性 (Transparency)」及「去連結性 (Unlinkability)」的隱私防護之目的及其間產生的競合關係 (例：可調解性與完整性) 等 (ISO 2018c)；以 ISO/IEC CD 27552.2 第 7.4.4~7.4.6 為例，PII 之資料去識別化的技術係採用「統計學技術」、「密碼學技術」、「抑制技術」、「擬匿名技術」、「概化技術」、「隨機化技術」、「數據合成技術」抑或「差分模型」、「K-匿名模型」？若採用「差分模型」，因其「伺服機模式」或「在地模式」於「資訊系統」之建置不同，亦須抉擇 (ISO 2018d; 吳英杰 2015)；表 4 及表 5 為擴增前述「軟體工程」與「隱私架構框架」宜考量的控制措施；表 6 及表 7 係闡明資訊系統供應鏈管理過程宜考量之隱私議題。

表 3 ISO/IEC CD 27552. 2 之 PII 控制者 PbD 的控制目標及控制措施 (ISO/IEC CD 27552. 2 附錄 A 第 7. 4 節)

A. 7. 4 從設計著手與以預設機制進行隱私防護		
目標：確保包含使用、保留、揭露、傳輸與處置 (Disposal) 的過程與系統，侷限於已識別之目的所必須之處理的設計。		
備考：同 ISO/IEC CD 27552. 2 第 7. 4 節，其實作指引及其他資訊宜參考之。		
A. 7. 4. 1	限制蒐集	控制措施 組織宜將 PII 的蒐集侷限於在攸關 (Relevant) 於其已識別之目的、成比例與必須之最小化。
A. 7. 4. 2	限制處理	控制措施 組織宜侷限 PII 的處理與其已識別之目的，適當、攸關且必須。
A. 7. 4. 3	正確性與品質	控制措施 在 PII 之生命週期中，組織宜確保與文件化其處理 PII 時，是正確、完整及最新的，並為目的之必須。
A. 7. 4. 4	PII 最小化與去識別化之目標	控制措施 組織宜定義與文件化，相對於已識別目的所須之程度是否需要將目標去識別化或最小化。
A. 7. 4. 5	PII 最小化與去識別化	控制措施 組織宜定義與文件化用於處理 PII 之設計的機制，其 PII 主體之 PII 能夠識別或關聯的程度符合第 7. 4. 4 建立之目標。
A. 7. 4. 6	在處理結束時 PII 去識別與刪除	控制措施 當原始 PII 不在需要用於其識別之目的，組織宜刪除 PII 或使其成為無法識別 PII 當事人之形式。
A. 7. 4. 7	暫存檔案	控制措施 組織宜確保在指定之文件紀錄的時限內依照文件化程序 (例：抹除或銷毀) 因處理 PII 而建立之暫存檔案。
A. 7. 4. 8	保存	控制措施 組織保存 PII 之時間不宜超過處理 PII 目的所需之時間。
A. 7. 4. 9	處置	控制措施 組織宜化將處置 PII 之政策、程序與機制文件化。
A. 7. 4. 10	PII 之傳輸控制措施	控制措施 組織對使用數據傳輸網路傳輸之 PII (例：送至其他組織) 進行適當控制，確保其資料到達預定目的地。

表 4 隱私工程設計之資料導向策略

名稱與描述	隱私控制措施例
最小化 (Minimize) : 盡量限制 PII 之處理。	<ul style="list-style-type: none"> 蒐集前先選擇 (Selection before collection)。 匿名 (Anonymization)。
分離 (Separate) : 盡量分開或隔離個人資料，以防止相關性。	<ul style="list-style-type: none"> 邏輯或實體分離 (Logical or physical separation)。 點對點約定 (Peer-to-peer arrangement)。 端點處理 (Endpoint processing)。
抽象化 (Abstract) : 當處理個人資料時，盡量限制細節是有助益的。	<ul style="list-style-type: none"> 隨時間之彙集 (Aggregation over time) 用於智慧電網 (Smart grids)。 動態位置粒度 (Dynamic location granularity) 用於基於位置之服務 (Location based services)。 K- 匿名 (K-anonymity)。
隱藏 (Hide) : 預防 PII 成為公開或已知 (Prevent PII from becoming public or know)。	<ul style="list-style-type: none"> 加密 (Encryption)。 混合 (Mixing)。 擾動 (Perturbation)(例如：差分隱私 (Differential privacy)、統計揭露控制 (Statistical disclosure control))。 去連結 (Unlinking)(例如：經由擬匿名化)。 屬性基存取控制信符 (Attribute based credentials)。
備考 1: 屬性基存取控制信符相關標準。	<ul style="list-style-type: none"> ISO/IEC 27551(制定中)。
備考 2: 去識別化相關標準。	<ul style="list-style-type: none"> ISO/IEC 20889。

表 5 隱私工程設計之過程導向策略

名稱與描述	隱私控制措施例
通知 (Inform) : 告知 PII 當事人關於 PII 之處理。	<ul style="list-style-type: none"> 隱私圖標 (Privacy icons)。 分層隱私政策 (Layered privacy policies)。 資料破口通知 (Data breach notification)。
控制 (Control) : 提供 PII 當事人控制其 PII 之處理。	<ul style="list-style-type: none"> 隱私儀表板 (Privacy dashboard)。 同意 (Consent)(包含撤回 (Withdrawal))。
執行 (Enforce) : 承諾 PII 處理是在一隱私友善方式之中，並貫徹執行。	<ul style="list-style-type: none"> 縝密之政策與隱私權管理 (Sticky policies and privacy rights management)。 隱私管理系統 (Privacy management system)。 資源之承諾 (Commitment of resources)。 指派權責人員 (Assignment of responsibilities)。
證明 (Demonstrate) : 證明是在一隱私友善方式之中處理 PII。	<ul style="list-style-type: none"> 日誌存錄與稽核 (Logging and auditing)。 隱私衝擊評鑑 (Privacy impact assessment)。 設計決策之文件 (Design decisions documentation)。
備考 1: 組織角色與其參照之標準。	<ul style="list-style-type: none"> PII 控制者、PII 處理者及供應商。 ISO/IEC/IEEE 15288(Systems and software engineering-system life cycle processes)。
備考 2: 隱私衝擊評鑑之參考標準。	<ul style="list-style-type: none"> ISO/IEC 29134。

表 6 隱私工程與系統生命週期過程

ISO/IEC/IEEE 15288 之過程類型 (Type of process)	隱私工程議題 (Privacy engineering issues)
協議過程 (Agreement processes) : 獲取過程 (Acquisition process) 。	涉及個人可識別資訊之供應鏈 (Supply chain involves PII) 。
協議過程 : 供應 (Supply) 過程 。	同上 。
組織之專案賦能過程 (Organizational project-enabling processes) : 人力資源管理過程 (Human resources management process) 。	隱私工程人力資源管理 (Privacy engineering human resource management) 。
組織之專案賦能過程 (Organizational project-enabling processes) : 知識管理過程 (Knowledge management process) 。	隱私工程知識管理 (Privacy engineering knowledge management) 。
技術管理過程 (Technical management process) : 風險管理過程 (Risk management process) 。	隱私風險管理 (Privacy risk management) 。
技術過程 (Technical process) : 利害關係人之需要與要求事項的過程 (Stakeholder needs and requirements process) 。	利害關係人之隱私期望 (Stakeholder privacy expectations) 。
技術過程 (Technical process) : 系統要求事項定義過程 (System requirements definition process) 。	隱私原則之運作 (Privacy principles operationalisation) 。
技術過程 : 架構定義過程 (Architecture definition process) 。	關注於隱私在架構上之衝擊 (Impact of privacy concerns on architecture) 。
技術過程 : 設計定義過程 (Design definition process) 。	隱私在設計上之衝擊 (Impact of privacy on design) 。

表 7 隱私工程與 VSE (Very Small Entities) 之系統生命週期過程

ISO/IEC 29110 之生命週期工作項目 (Artefacts)	隱私工程議題 (Privacy engineering issues)
獲取方 (Acquirer) : 工作 明書 (Statement of work) 。	同左 。
獲取方 : 產品 (Product) 。	產品之隱私能力 (Product with privacy capabilities) 。
組織管理 (Organizational management) : 外部實體 (External entity) 。	隱私工程人力資源管理 (Privacy engineering human resource management) 。
計畫管理過程 (Project management process) : 風險管理活動 (Risk management activity) 。	隱私風險管理活動 (Privacy risk management) 。
系統定義及其實現過程 (System definition and realization process) : 系統定義及其實現起動 (Initiation) 。	利益相關者之隱私期望活動 (Stakeholders privacy expectations activity) 。
系統定義及其實現過程 : 系統要求事項工程 (System requirement engineering) 。	隱私原則之運作 (Privacy principles operationalization) 。
系統定義及其實現過程 : 系統架構設計 (System architectural design) 。	隱私工程架構活動 (Privacy engineering architectural activity) 。
同上 。	隱私工程設計定義活動 (Privacy engineering design definition activity) 。
系統定義及其實現過程 : 系統建構活動 (System construction activity) 。	人力資源管理 (human resource management) 。

綜前所述，雲端運算服務 PbD 的「預設機制防護隱私」之框架如圖 4 所示 (Intel 2017; ISO 2013; TCG 2018)；確保諸如「抹除」於設計處理過程中「以預設機制適當的防護隱私」等，則為「聚焦於資訊公開與個人隱私衡平之議題，發掘 PII 處理過程在資訊系統可能發生的不能接受後果之系統工程」的「隱私工程」之標的 (ISO 2018c; ISO 2018e; ISO 2018g)，惟囿於篇幅未討論其實作。

肆、結論

標準可以累積知識與經驗，標準化則是冀求以系統的、共同的、協調一致的方法來強化標準實作之知識以供傳承。」15 年來，我國 ISMS 與 PIMS 的實作卻以通過驗證為標的，致使事倍功半，前述誤將「刪除」之規範作為前述 ISO/IEC 27018 中，「抹除」的驗證標準即為例證。GDPR 之 PIMS 標準化之研究與實施必須設法超越彷彿不證自明的 ISMS 之驗證與認證空間，使其成為資訊社會的基石；我國在 2000 年前後形成之 ISMS 驗證的空間，是不同利益之行動者追求商業利益，將其「挪為己用」的「經營」而形成之，其「租值消散 (Dissipation of rent)」的情境已顯現之 (中華民國資訊軟體協會 2012; 許瀞文 2013)。政府是對個人資料保護有監督管理權責的行政機關之管理的當責 (Accountability) 實體，做為一個控制 PIMS 規範之集中式權力機構，其對 PIMS 驗證的觀點影響到 PIMS 標準化之進程；歐盟與美國的經由規範以及評鑑與測試 ISMS 及 PIMS「行為準則」之遵循 (Official

Journal of the European Union 2016; ISO 2018a; ISO 2018b; ISO 2018c; ISO 2018d; ISO/IEC 2018e; OMB 2016)，及其經由法規制約諸如「抹除」、圖 4 中的如何將隔離及完整性之概念擴增至其應用的資訊實體 (Cyberphysical) 之中、隔離與完整性之集中性管理與元資料 (Metadata) 分散式的資料管理 (例：台電第三代電能管理系統防範 729 與 921 停電事件的方案 (許志義等 2000; 鄭金龍等 2005; Wong et al., 2007)) 之 PbD 等 ISMS 及 PIMS 的控制措施適足性之標準化 (何念修 2019b)，值得我們借鏡。

致謝詞

作者謹在此匿名審稿者提升本文內容水平之意見，致衷心的謝忱。

參考文獻

1. 中國國家標準化管理委員會，2017，信息安全技術 個人信息安全規範，GB/T 35273(報批稿)。
2. 中華民國資訊軟體協會，2012，行政院「完備我國資訊安全管理法規之分析」委託研究計畫期中報告 (初稿)，頁 88(法務部資訊處前陳泉錫處長 2012-07-27 之訪談紀錄)。
3. 何念修，2019，個資保護「適當之安全措施」-以新加坡個資法之技術措施建議為比較對象，科技法律透析，第 31 卷，第 1 期，頁 55~61。
4. 吳英杰，2015，隱私保護數據發布：模型與算法，清華大學出版社。

5. 紀珮宜，2017，由歐盟資料保護規則論被遺忘權之爭議，經貿法訊第 214 期 (2017- 05- 25)，頁 8~ 24。
6. 財團法人金融聯合徵信中心，2017，歐盟個人資料保護規則，金融徵信叢書，NO. 77。
7. 許志義等，2000，從「七二九」與「九二一」停電事件分析我國電力系統之安全政策行政院研究發展考核委員會。
8. 許靜文，2013，花錢就能拿證書 台灣資安玩假的？，今週刊，頁 54~ 56。
9. 鄭金龍等，2005，台電中央調度中心分散型電能管理系統的規劃與建置，台電工程月刊，第 688 期，頁 77~ 88。
10. ABAC(Attribute Based Access Control), 2019, 2019- 02- 17 檢 索， 取 自 <http://nccoe.nist.gov/forums/attribute-based-access-control>.
11. ACM, IEEE-CS, AIS SIGSEC and IFIP WG 11. 8, 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Version 1. 0 Report, 2017- 12- 31.
12. Brito, A., editor, 2017, Secure Cloud, Analysis of existing technologies, 2019- 03- 18 檢 索， 取 自 <http://www.securecloudproject.eu/wp-content/uploads/D 2. 1-final.pdf>.
13. Chatila, R., editor, 2019, Ethically Aligned Design, First Edition, IEEE Standards Association.
14. Common Criteria, 2019, 2019/ 03/ 05 檢 索，取自 <http://www.commoncriteriaportal.org>.
15. ENISA, 2014, Privacy and Data Protection by Design-from policy to engineering, 2014- 12.
16. EuroPriSe, 2017, EuroPrise Criteria for the certification of IT products and IT-based services (“ GDPR ready ” version-January 2017).
17. Grassi, P. A., Lefkovitz N. B., Nadeau E. M., Galluzzo R. J. and Dinh A. T., 2018, Attribute Metadata, Proposed Schema for Evaluating Federated Attributes. NIST Internal Report 8112, 2018- 01.
18. Hughes, Gordon, and Tom Coughlin, 2006, "Tutorial on disk drive data sanitization." 2017/ 9/ 30 檢 索， 美 國 聖 地 牙 哥 加 州 大 學 (University of California San Diego)， 取 自 https://cmrr.ucsd.edu/_files/data-sanitization-tutorial.pdf.
19. Intel, 2017, Intel TXT(Intel Trusted Execution Technology) Software Development Guide, Revision 015, 2017- 11.
20. ISO, 2013, ISO/IEC 29101: 2013- 10- 15, Information technology – Security techniques – Privacy architecture framework.
21. ISO, 2014, ISO/IEC 27018: 2014- 08- 01, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
22. ISO, 2015a, ISO/IEC 27040: 2015- 01- 15, Information technology – Security techniques – Storage security.

- 23.ISO, 2015b, ISO/IEC 27017: 2015- 12- 15, Information technology – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- 24.ISO, 2015c, ISO/IEC 11889: 2015(E), Information technology – Trusted platform module library(Part 1~ 4).
- 25.ISO, 2016, ISO/IEC 19086- 1: 2016- 09, Information technology – Cloud computing – Service level agreement (SLA) – Part 1:Overview and concepts.
- 26.ISO, 2017, ISO/IEC 19086- 3: 2017- 07, Information technology – Cloud computing – Service level agreement (SLA) – Part 3: Core conformance.
- 27.ISO, 2018a, ISO/IEC CD 27552. 2: 2018- 06- 04, Information technology – Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements.
- 28.ISO, 2018b, ISO/IEC 19896- 3: 2018- 03- 01, IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements.
- 29.ISO, 2018c, ISO/IEC 2nd PDTR 27550: 2018- 06- 04, Information technology – Security techniques – Privacy engineering for system life cycle processes.
- 30.ISO, 2018d, ISO/IEC 20889: 2018- 11, Information technology – Security techniques – Privacy enhancing data de-identification terminology and classification of techniques.
- 31.ISO, 2018e, ISO/IEC 24748- 1: 2018- 11, System and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.
- 32.ISO, 2018f, ISO/IEC JTC 1/SC 27 N 17896, 2018- 01- 10, Text for WG 5 Standing Document 1(SD 1)-WG 5 Roadmap.
- 33.ISO, 2018g, ISO/IEC TS 19608: 2018- 10- 15, Information technology – Security techniques – Guidance for developing security and privacy functional requirements based on ISO/IEC TS 15408.
- 34.ISO, 2019a, ISO/IEC TS 27008: 2019, Information technology –Security techniques –Guidelines for the assessment of information security controls.
- 35.ISO, 2019b, ISO/IEC 27701: 2019, Information technology –Security techniques –Enhancement to ISO/IEC 27001 for privacy management –Requirements.
- 36.ITU, 2016, 12th Revision of Cloud Computing Standards Roadmap on December 2015, Study Period (2013~ 2016), Study Group 13, TD 502(WP 2/ 13).
- 37.Kissel, R. et al., 2014, Guidelines for Media Sanitization, NIST SP 800- 88 Revision 1.
- 38.Official Journal of the European Union, 2016, General Data Protection Regulation (GDPR), REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.
- 39.OMB, 2016, Annual Report to Congress: Federal Information Security Modernization Act.

40. Rannenbergh, K., 2017, Privacy Management Data Protection Standardization(Presentation), in CEN-CENELEC-ENISA workshop, Cybersecurity and Data Protection Standards in support of European policy, 2017- 09- 19, Brussels, Belgium.
41. TCG(Trusted Computing Group), 2018, 2018/ 12/ 19 檢 索， 取 自 <http://www.trustedcomputinggroup.org>.
42. Willett, M., 2009, Self-Encryption Drives, 2017/ 9/ 30 檢 索， 全 球 網 路 存 儲 工 業 協 會 (Storage Networking Industry Association)， 取 自 http://www.snia.org/sites/default/education/tutorials/2009/fall/security/WillettMichael-Self_Encryption_Drives-FINAL.pdf.
43. Yeluri, R. and Castro-lean E., 2014, Building the Infrastructure for Cloud Security-A Solutions View, Apress, 2015/ 01/ 17 檢 索， 取 自 <http://www.apress.com/br/book/9781430261452.pdf>.
44. Wong, J-J et al., 2007, Study on the 729 blackout in the Taiwan power system, Electrical Power & Energy Systems, 29, 589~ 599.

Cybersecurity and AI — Implications for Internal Auditing

Toshifumi TAKADA

Professor, National Chung Cheng University, Taiwan

E-mail: ttakada0830@gmail.com

Masatoshi SAKAKI

Partner, EY Shinnihon Audit Firm, Japan

E-mail: masatoshi.sakaki@jp.ey.com

Shiro, AOYAGI

CEO, Global Security Expert Inc, Japan

E-mail: saoyagi@gsx.co.jp

Hiroshi, KAWAGUCHI

CEO, Kawaguchi Sekkei Inc., Japan

E-mail: kawa@sec-k.co.jp

Abstract

Computer system now is facing risks of attacking and destroying it. Such illegal actions are caused by hackers; they are people with IT knowledge. They are individuals in some incidents but it is reported that they are trained by the government. They attacked computer systems and stole assets, confidential information, higher technology, etc. In addition to this, many governments are concerned that they attack infra-structure's computer systems; for example, power plants, traffic control systems, police and military computer systems, etc. How can we safeguard the computer systems from such malicious attack? This issue is called Cybersecurity. The authors are thinking Cybersecurity education

is one of the most effective solutions and we are engaged in the education. And we made a proto-type AI program (Supervised Machine Learning) to detect attacking before computer systems were destroyed. Our conclusion is that combination AI and Cybersecurity education is very effective to safeguard the computer system. Many companies have noticed the necessity of Cybersecurity but they don't have a department specialized in it. We have proposed that internal audit department shall be responsible for this duty.

Keywords: AI, Supervised machine learning, Internal auditor, Cybersecurity, Hackers, Incidents

I. INTRODUCTION AND OBJECTIVES

1- 1. Introduction

Computer crimes happened in 1970s. These crimes were serious for the companies but they were isolated within companies. But this condition changed dramatically when the Internet age started in 1990s. All the computers in the world are connected and this means that the computer systems are connected with outside networks. Hackers can enter the computer system much easier than before.

In addition, it is reported that a few countries have trained professional hackers in the government. They are professional hackers and steal secret information, valuable

assets and intervene political actions, etc. Many governments have recognized this issue and they also take actions against these illegal behaviors. The followings are main actions by the Japanese Government in these 5 years.

- (1) The Japanese Government enacted "The Basic Act of Cybersecurity" Act No. 104, in November 12, 2014.¹
- (2) Ministry of Internal Affairs and Communications, Japan, disclosed "WHITE PAPER" every year. In 2018 version, their concerns about Cybersecurity were demonstrated.²
- (3) National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was organized in 2017. They are national center of Cybersecurity and they issued "Information Security

1. The Japanese Government, The Basic Act of Cybersecurity, Act No.104, November 2014.

<http://www.japaneselawtranslation.go.jp/law/detail/?vm=04&re=01&id=2760>

The Japanese Government has made policies of Cybersecurity based on this act. NISC is organized by this act.

2. Ministry of Internal Affairs and Communications, Japan, Information and Communications in Japan, WHITE PAPER, 2014-2018.

<http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/2018-index.html>

This Ministry is responsible for making and executing Cybersecurity policies.

Handbook for Network Beginners”
V.2.11e. and other documents.³

- (4) National Institute of Information and Communication Techniques (NICT) opened the training center called Cyber Defense Exercise with Recurrence (CYDER) and started education for Cybersecurity.⁴

CYDER is a public organization funded by the Japanese Government. The number of trainees is limited. Cyber education in private sector is also needed such as Global Security Experts Inc.(GSX)

The authors have been engaged in Cybersecurity education since 2015. Takada and Sakaki are teaching Cybersecurity and auditing in universities; Aoyagi and Kawaguchi are teaching Cybersecurity at GSX. We had an opportunity to collaborate with each other and decided to make a presentation at an international conference and to submit our paper to a journal. This paper is the result of our collaboration. This paper is not an empirical study but is oriented to the field study at the education of GSX and to make a prototype of AI program in the field of Cybersecurity. We have a very clear vision of

making a useful tool to the practice.

1- 2. Objectives

There are 3 objectives of this paper. They are

- (1) To do a statistical test about the effects of Cybersecurity education:

One of the largest security issues is Cybersecurity. As all the computers and sensors are connected to each other by Internet, anyone can access computer systems via Internet. Computers are protected by security software and it requires ID and PW to enter the system. On the other hand, sensors don't have strong security system. Hackers can easily enter sensors and destroy the system or cause malfunctions of connected machines. Many governments notice this and they organize the organizations for Cybersecurity.

Our objective of this paper is to do statistical test whether or not educations of Cybersecurity are effective. 2 authors of this paper, Shiro Aoyagi, CEO of Global Security

3. National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Information Security Handbook for Network Beginners, V.2.11e, 2017.

https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf

NISC has been organized and funded by the Ministry of Internal Affairs and Communications, Japan. NISC is active in Cybersecurity. This Handbook can be downloaded from the NISC website.

4. National Institute of Information and Communication Technology (NIST), Cyber Defense Exercise with Recurrence (CYDER), 2017.
<https://cyder.nict.go.jp/>

CYDER is a national training center for Cybersecurity. The courses held by CYDER is similar to Micro Hardening; 4 students in a team, using realistic incidents, to learn how to protect computer system from attacking.

Experts Inc. (hereafter GSX)⁵, and Hiroshi Kawaguchi, CEO of Kawaguchi Sekkei Inc.⁶, are leaders in the education of Cybersecurity company. Data in this paper was collected by them.

GSX has made an educational service to the client companies about Cybersecurity. They made a questionnaire survey from the students attending the courses of Cybersecurity. We found GSX education was very effective. One of the most effective methodologies of Cybersecurity is to educate personnel in the IT department of a company. GSX has responded customer's many Cybersecurity incidents.

(2) To make prototype AI programs for Cybersecurity:

Even if education is effective, it is impossible to protect computer system perfectly from attacking by hackers. Targeted Email Attacking Training is very effective but some percentage of personnel opens a suspicious email with malware. Before being attacked, safeguarding measures had better be installed. One of them is AI program to

detect attacking. AI is a computer program and it doesn't cause a human error.

(3) To consider implications to internal auditor

After having detected attacking, computer systems must be protected from it and the attacking must be reported to top management. Cybersecurity has become a very serious issue for a company, organization, government and society. Top managements and leaders need to take actions against attacking to computer system. Many companies have an internal audit department and the report of this department ordinarily addressed to top management. Unfortunately, internal auditors don't have enough knowledge about Cybersecurity and they don't have contacts with information department. This present condition must be improved immediately. We will make several implications for internal auditors.

1- 3. Literature Review

Several countries have noticed the

5. Global Security Experts Inc.(GSX) <https://www.gsx.co.jp/>

GSX was launched as a group company of Business Brain Oota Showa. Now it is specialized in the education of Cybersecurity. They offered several courses; Targeted Email Attacking Training, Micro Hardening, Certified Network Defender (CND), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), etc.

6. Kawaguchi Sekkei Inc. <https://www.sec-k.co.jp/>

Mr. Hiroshi Kawaguchi has started Kawaguchi Sekkei Inc. in 2018. He is a specialist of Micro Hardening and has a collaboration with GSX. He is an instructor of this course.

importance of cybersecurity by increasing incidents in recent years. Some incidents are said to be caused by the military departments by a few countries. The Taiwanese and Japanese Government have enacted laws and rules related to cybersecurity. We surveyed official documents issued by the Japanese Government. They have started cybersecurity education but the classrooms are too small to satisfy the increasing needs.

We also surveyed academic articles published by journals and issued by organizations. To detect attacking beforehand needs tools (computer programs). Many authors indicated that (1) software for computer aided audit techniques such as ACL or IDEA is too general to detect attacking by hackers those days. (2) SMEs' CEOs need to understand the necessity of cybersecurity. (3) SMEs don't have a department responsible for cybersecurity. (4) Specialized software for current incidents has not been developed yet.

Authors have recognized the emergency condition of cybersecurity as the governments and many authors. GSX has accumulated experiences through cybersecurity education. One of the authors is Mr. Aoyagi, CEO of GSX, and we collaborate to each other to deal with this issue.

II. CYBERSECURITY EDUCATION COMPANY AND ITS COURSES

2-1. Targeted Email Attacking Trainings

Targeted email attack is defined as attack to specified person(s) computer in a company by email with malware. If the person clicks the email, its computer is infected by a malware and hacker can override the computer and steal information from host computer system. GSX has started educational training of targeted email attacking since 2013. A person had an experience of targeted email attacking twice and he/she will become much more careful at the 2nd session than the 1st session.

The subjects and percentage of opening the targeted attacking email were as follows.

Construction Industry

- | | |
|------|--|
| 2015 | First: [Caution] About influenza, 16.9% |
| | Second: [Emergency] Security information of Windows: 8.0% |
| 2016 | First: [Urgent] Asking email box: 46.5% |
| | Second: Sharing incident of information leakage: 33.4% |
| 2017 | First: How to improve the response speed of Internet: 23.7% |
| | Second: [Confirmation] Notice of your medical expense: 45.8% |

2018 First: [Confirmation] Notice of your credit card use of this month: 19.2%

Second: [Urgent] How to improve the response speed of Internet: 17.8%

Table 1. Results of Targeted Email Attacking Training

	2015		2016		2017		2018	
Industry	First	Second	First	Second	First	Second	First	Second
Schools	13.5	12.4	21.6	26.5	2.4	7.6	8.7	6.7
Finance			26.5	3	7.5	4.7	1.2	1.2
Retail					21.6	15.5	32	24.2
Manufacturing	26.5	16.6	12	26.2	21.2	10.8	14.5	3.8
Significance level = 95%, $Z \geq 1.96$								

There are 3 second training sessions (in red) were higher than the first training session but generally the percentage of second became lower than the first. It is the effect of education held between the first and the second training.

We tested this result as follows.

Number of training: 17 (=n), First > Second: 13, Null hypothesis: $p = 0.5$, Level of significance = 0.05 $Z_{0.05} = 1.96$ (both sides)

$$\begin{aligned}
 Z &= (13 - 17 \times 0.5) / \text{square root} (17 \times 0.5 \times (1 - 0.5)) \\
 &= 4.5 / 2.06 \\
 &= 2.18 > 1.96
 \end{aligned}$$

We can reject null hypothesis. Therefore, we can say that the percentage of opening an email with malware at the 2nd training session is lower than the 1st training session. This means that education is effective; students are more careful at the 2nd targeted email.

Targeted email attacking has been a traditional method of hacking. Everyone knows its risk but many people click such email with malware. Very serious information leakages were reported every year even for large companies. For example, JTB (Japan Travel Bureau, 2016), JPS (Japan Pension Service, 2015)⁷, JAL (Japan Air Line, 2014), etc. An employee carelessly opened a targeted attacking email with malware and a hacker made a backdoor of the main computer and stole customer information from host computer.

2-2. Micro Hardening

Micro Hardening is a computer simulated educational training developed by Mr. Kawaguchi, CEO of Kawaguchi Sekkei Inc. GSX has a Micro Hardening training course collaborated with Kawaguchi Sekkei. 4 students make a team and the mission of a team

7. National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Report of the Investigation on Causes of Leakage of Japan Pension Service, 2015.

https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

This was a big incident of private information leakage. Personnel of Japan Pension Service are using PCs in the office connecting to Internet. Hackers overrode these PCs and stole lots of private information.

according to the following method.

(1) Each team has E-commerce shop. The shop will be attacked by hackers. Examples of incidents are as follow.

(a) Weak, simple password which are easily stolen by hackers.

(b) Entering the website of supervisors

(c) Access to the files of a shop with weak protection

(2) Mission of a team is to maximize sales of shop and to maximize the points of successful protection from attacking. If the protection is very rigid, the ordinal consumers can't enter the shop resulting in the very small sales.

(3) There are 3 sessions in a training day. Each session is 45 minutes.

Table 2 shows the result of 3 sessions.

Table 2. Effects of Micro Hardening			
	1st Session	2nd Session	3rd Session
Sales	68,302	82,778	94,639
SD	15,489	27,382	31,066
Z-score		6.87	4.96
Points	5.98	8.5	10.29
SD	3.09	3.24	3.04
Z-score		10.08	7.65
Significance level =95%, $Z \geq 1.96$			

Number of teams were 169. We used one sided Z-test as the number is large enough. Average Sales of a shop and Points for protection are becoming larger from 1st session to the 2nd session, from the 2nd session to the 3rd session. Each Z-score is larger than 95% significance level 1.96.

We conclude that we can reject null hypothesis and that Micro Hardening has effects evidently. Micro Hardening is a very practical educational training as it uses many incidents occurred previously.

III. AI PROGRAM FOR CYBERSECURITY

AI is now widely used in many companies. It will also play an important role in Cybersecurity to detect attacking. We human being react against the stimulus from outside. We tend to take subjective behaviors and as a result, it is impossible to escape to be deceived by hackers. As Table 1 shows, even after the 1st session, many students opened the targeted email at the 2nd session. And 3 cases, 2nd session became worse than 1st session.

Computer program is very rigid and objective. AI program is superior to traditional program in speed and flexibility. We made 3 prototype AI programs to detect irregularity. These can be applied to detect a suspicious email and illegal access to the computer.

3- 1. Short history of AI

The development of Artificial Intelligence (AI) was initiated in 1980s. Prolog, LISP and a few programming languages and tools were used to make AI programs. AI programs are consisted of inference engine and knowledge base. In the field of professional judgment, Expert System was thought to be applied as a decision aid for professionals. Unfortunately, the boom of AI in 1980s ended in 10 years. There were several reasons for this AI boon going down.

One of the main reasons was thought to be the limitations in the performance of computer hardware at that time. Expert System was intended to substitute a highly experienced professional's way of thinking by computer. An experienced professional accumulated huge amount of knowledge. Even if AI programmers could extract's know-hows and put them into AI's knowledge base, it was difficult for a hardware of computer to execute programs to get useful answer in a few seconds. In addition to this, the computer was expensive and very big. High performance PC at that time was over 5,000 US\$. It was difficult to use such expensive computers for AI.

On the other hand, Research in AI in

1980s demonstrated the possible development in the future. We had a dream to develop AI if the computer when cost-performance of a computer were improved. AI is different from a traditional computer programs in that it has a flexibility to expansion of human knowledge. Knowledge of professionals is increasing rapidly day by day and year by year. Practitioners accumulate their knowledge through practice and experience. AI is capable to import such growing knowledge. We are now standing at the threshold of incorporating AI into practice.

Now price of hardware of computer became lower and lower, AI can be applied to the decision aid for professional decision in many fields. Professional standard now requires highly sophisticated judgment and decision for professionals. AI can substitute the professional judgment on behalf of them. We are thinking AI programs can detect suspicious emails and irregular access to the computer system and files much more efficiently than human.

3- 2. Outline of Supervised Machine Learning

In this paper, we made prototype AI programs to detect attacking by hackers. We use the "Supervised Machine Learning" for this purpose.

Supervised Machine Learning (SML) can be applied for this purpose. SML is one of the AI programming techniques. It is a simple program. "Supervised Machine" means that

the program has a standard to judge Yes or No. Judgment of Yes or No is a grouping of A and B or Classification of A and B. Here we use 3 models; Discriminant Model, Maximum Likelihood Estimation and Logistic Linear Regression Model. Standard is a boundary line or a boundary point which isolate A from B. AI program which minimizes the mistaken grouping of A and B is the best one.

3- 3. One Dimensional Data and Classification problem

To focus the problem clearly, we assume the following conditions.

- (1) We generate data by using simulation technique. The data is one dimensional data.
- (2) We also generate data A as 0 and B as 1 and the probability of A is 0.5 and B is 0.5. We assume the probability is 0.5 for each group because of simplification.
- (3) Both group A and B has a normal distribution or uniform distribution. A ranges from 0.9 to 2.0 and B ranges from 0 to 1.0. A is known to belong to attacking data; B belongs

to the ordinary data.

3- 4. Discriminant Model

Discriminant model is a multivariate liner discriminant model to grouping A and B. A group are consisted of attacking data and B group are consisted of ordinary data. Each group is assumed to have a normal distribution. Discriminant model tells the discriminant point of A and B. The discriminant point can be used to group A or B. There is a risk to make a mistaken judgement of A group as B group and vice versa because A group' s distribution is crossing B group' s distribution. The crossing point is where we can minimize the number of error judgment.

We assume both A and B has the same normal distribution. Crossing point is the center of the crossing zone. For example, if the crossing zone is from 0.9 to 1.3, crossing point can be calculated

$$(0.9 + 1.3) / 2 = 1.1$$

The result of simulation will be shown by the Python program as follows.

IV.IMPLIMENTATION OF AI PROGRAM

Discriminant Model

```
# Python Program for Discriminant Model
import numpy as np
import matplotlib.pyplot as plt

# Simulated Data Generation
```



```

np.random.seed(seed= 3)                                #Fix data with other programs

#Initialization of data and array
X_min = 0
X_max = 2. 5
X_n = 100
X = np.zeros(X_n)                                       #Score of Companies
T = np.zeros(X_n, dtype=np.uint 8)                     #Target Data
Dist_s = [ 0. 4, 0. 8]                                  #Initial data for each group
Dist_w = [ 0. 8, 1. 6]                                  #Range of data A: 0. 4 to 0. 8; B: 0. 8 to 1. 6
Pi = 0. 5                                                #Percentage of each group

#Simulated Data Generation
for n in range(X_n):
    wk = np.random.rand()
    T[n] = 0 * (wk < Pi) + 1 * (wk >= Pi)                #Group A
    X[n] = np.random.rand() * Dist_w[T[n]] + Dist_s[T[n]] #Group B

# Show Result
print('X= ' + str(np.round(X, 2)))
print('T= ' + str(T))
print('Bondary = ' + str(np.round(np.median(X), 2)))

```

The result of the program above is as follows.

Simulated number of companies = 100

Boundary = median = 1. 08

Score of A < median; Score of B >= median

V. ROBUSTNESS TESTS OF AI PROGRAMS

We did 2 robustness tests of AI Discriminant Model; (1) Maximum Likelihood Estimation and (2) Logistic Linear Regression Model. The result is as follows.

5- 1. Maximum Likelihood Estimation

Maximum Likelihood Estimation uses the probability. We know the number of occurrence 0 and 1 in the field of crossing zone. For example, if there are totally 10 occurrences in the crossing zone between 0. 8 and 1. 2 (6 zeros and 4 ones), then the probability of zero is $6 / 10 = 0. 6$. This 0. 6 is called Likelihood.

Most Likelihood Estimation is proved as follows.

$$P(t=1 | x) = w \quad \text{where } a < x \leq b$$

If $T = (0|n) \times (1|m)$ then

$$P(T=(0|m) \times (1|n) | x) = [(1-w)]^m \times w^n$$

$$\log_{f_0} [P = \log \{(1-w)^m w^n\}] = m \log_{f_0} (1-w) + n \log_{f_0} w$$

$$\partial / \partial w \log_{f_0} [P = \partial / \partial w [m \log_{f_0} (1-w) + n \log_{f_0} w] = 0]$$

$$m(-1)/(1-w) + n(1/w) = 0$$

$$(-mw + n - nw)/(1-w)w = 0$$

$$-mw + n - nw = 0$$

Consider there are 10 companies in the crossing zone. We can say that 6 of them are belonging to A group and 4 of them are belonging to B group.

The point is calculated by $P(t=1|x) = 0.4$.
 $\therefore x = 1.23$ Python program below will show this calculation.

5-2. Logistic Linear Regression Model

We assume the distributions above are normal distribution and uniform distribution but data don't fit the distributions. The curve by logistic linear regression model is

fitting much better than other models. This curve looks like a slope curve between 0 and 1. Crossing point of logistic linear regression model is a boundary of A from B.

Suppose a logistic linear regression model as: $y = \sigma(w_0 + w_1 x)$

The function of a curve is as:
 $\sigma(x) = 1 / (1 + \exp(-x))$

Regression model of y is a straight line and the curve is a slope curve line between 0 and 1. Crossing point shows a boundary of A from B and it is 1.25 calculated by Python program below.

5-3. Implementation of Maximum Likelihood Estimation

Python Program for Maximum Likelihood Estimation

import numpy as np

import matplotlib.pyplot as plt

Simulated Data Generation

np.random.seed(seed=3)

#Fix data with other programs

```

#Initialization of data and array
X_min = 0
X_max = 2.5
X_n = 100
X_col = ['red', 'gray']
X = np.zeros(X_n)
T = np.zeros(X_n, dtype=np.uint8)
Dist_s = [0.4, 0.8]
Dist_w = [0.8, 1.6]
Pi = 0.5 #Percentage of each group

#Score of Companies
#Target Data
#Initial data for each group
#Range of data A: 0.4 to 0.8; B: 0.8 to 1.6

#Simulated Data Generation
for n in range(X_n):
    wk = np.random.rand()
    T[n] = 0 * (wk < Pi) + 1 * (wk >= Pi)
    X[n] = np.random.rand() * Dist_w[T[n]] + Dist_s[T[n]]

# Show Data
print('X= ' + str(np.round(X, 2)))
print('T= ' + str(T))

#Show Uniform Distribution
def show_data_1(x, t):
    K = np.max(t) + 1
    for k in range(K):
        plt.plot(x[t == k], t[t == k], X_col[k], alpha=0.5, linestyle='none',
                 marker='o')
plt.grid(True)
plt.ylim(-.5, 1.5)
plt.xlim(X_min, X_max)
plt.yticks([0, 1])

# Show Boundary
fig = plt.figure(figsize=(3, 3))
show_data_1(X, T)
plt.show()

```

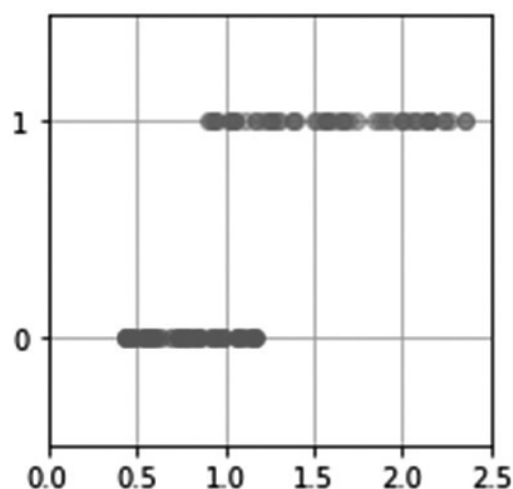
The result of the program Maximum Likelihood Estimation is

X= [1. 93 0. 81 2. 23 0. 57 0. 75 0. 77
1. 25 1. 75 0. 85 0. 73 0. 95 0. 53 2. 05 0. 58
1. 15 1. 88 2. 15 0. 47 1. 69 0. 58 0. 78 0. 63
1. 09 1. 25 0. 76 0. 56 0. 94 0. 69 1. 99 1. 9
0. 93 0. 86 0. 76 0. 59 1. 17 1. 84 1. 56 0. 91
0. 56 0. 48 0. 84 1. 16 1. 67 1. 22 2. 14 1. 57
1. 99 2. 26 1. 39 1. 11 0. 98 2. 36 1. 67 0. 79
2. 06 0. 76 0. 54 1. 11 1. 03 0. 44 0. 98 1. 57
0. 92 1. 5 0. 45 1. 17 2. 14 0. 61 2. 23 0. 45
1. 27 1. 05 2. 15 1. 37 1. 02 0. 74 1. 05 2. 08
1. 39 0. 59 2. 34 1. 57 1. 07 0. 95 1. 07 1. 3
0. 74 0. 95 1. 66 1. 17 2. 16 2. 14 0. 44 1. 29
1. 05 1. 6 0. 92 0. 45 1. 51]

T= [1 0 1 0 0 0 1 1 0 0 0 0 1 0 0 1 1 0 1 0
0 0 0 1 0 0 1 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1

1 1 1 1 1 0 1 1 0 1 0 0 0 1 0 0 1 0 1 0 0 1 0 1 0
1 1 1 1 1 0 1 1 1 0 1 1 0 1 0 1 0 1 1 1 1 0 1 0 1
1 1 1 0 1]

The probability of attacking is $P(t=0|x)=1-P(t=1|x)$ where $x=1.24$



5- 4. Implementation of Logistic Linear Regression Model

Python Program for Logistic Linear Regression Model

import numpy as np

import matplotlib.pyplot as plt

Simulated Data Generation

np.random.seed(seed= 3)

#Initialization of data and array

X_min = 0

X_max = 2. 5

X_n = 100

X_col = ['red', 'gray']

X = np.zeros(X_n)

T = np.zeros(X_n, dtype=np.uint 8)

Dist_s = [0. 4, 0. 8]

Dist_w = [0. 8, 1. 6]

#Fix data with other programs

#Score of Companies

#Target Data

#Initial data for each group

#Range of data A: 0. 4 to 0. 8; B: 0. 8 to 1. 6

```

Pi = 0.5                                #Percentage of each group

#Simulated Data Generation
for n in range(X_n):
    wk = np.random.rand()
    T[n] = 0 * (wk < Pi) + 1 * (wk >= Pi)    #Group A
    X[n] = np.random.rand() * Dist_w[T[n]] + Dist_s[T[n]]    #Group B

# Show Data
print('X= ' + str(np.round(X, 2)))
print('T= ' + str(T))

#Show curve
def logistic(x, w):
    y = 1 / ( 1 + np.exp(-(w[ 0] * x + w[ 1])))
    return y

# Show Logistic Linear Regressio Function
def show_logistic(w):
    xb = np.linspace(X_min, X_max, 100)
    y = logistic(xb, w)
    plt.plot(xb, y, color='black', linewidth= 3)
    # Boundary
    i = np.min(np.where(y > 0.5))    #A group
    B = (xb[i - 1] + xb[i]) / 2    #B group
    plt.plot([B, B], [-.5, 1.5], color='k', linestyle='--')
    plt.grid(True)
    print(str(B))
    plt.show()
    return B

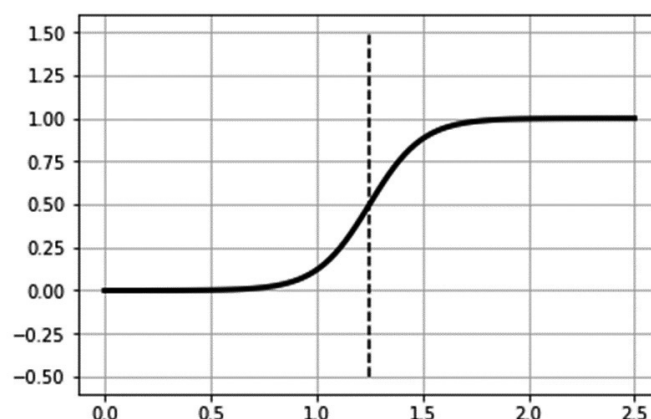
#Trial
w = [ 8, - 10]
show_logistic(w)

```


The result of Program above is

1. 25

The boundary is 1. 25.



4- 4. Comparison of each method and Robustness Test

We simulated 3 methods to evaluate the ability of detection of attacking; Discriminant Model, Maximum Likelihood Estimation and Logistic Linear Regression Model. The results (boundaries) of each Python program were 1. 08, 1. 24 and 1. 25.

The performance of these models can be evaluated by the number of errors; wrong classification of attacking data from ordinal data and vice versa. We need to know the real number of attacking to calculate scores and to group them by using 1. 08 (variable depending on the sample), 1. 24 and 1. 25. As we don't have the real attacking data, we have to use simulation. We assume the followings.

Scores range between 0. 4 to 2. 5.

Score of crossing zone of attacking (A) and ordinal (B) is between 0. 8 and 1. 2.

Probability of A is 0. 5 and B is 0. 5 in the crossing zone.

The result is as follows.

Discriminant Model case where possible number of errors of crossing zone is between 0. 8 and 1. 13: 10

Maximum Likelihood Estimation (0. 8 to 1. 24): 13

Logistic Model (0. 8 to 1. 25): 14

Discriminant Model got the lowest number of errors because the boundary was lower than other 2 methods. Discriminant Model assumes that both A group and B group has normal distribution. Distribution of real data or simulated sample data doesn't fit normal distribution.

The results of Maximum Likelihood

Estimation and Logistic Linear Regression Model were almost similar. Maximum Likelihood Estimation assumes uniform distribution of 0 and 1.

We did robustness test. This test was done by changing random seed and number of samples and applied to the Python program generating simulated data. The performance of robustness tests was Discriminant Model >

Maximum Likelihood Estimation > Logistic Model.

We need to consider the data fitting with each method. We have no evidence about the existence of normal distribution and uniform distribution. These distributions are used for the simplification of explanation. Simulated data is best fitting with the curve moving from 0 to 1.

Table 3. Results of Robustness Tests

Trial #	Seed	Sample Size	Discriminant	MLE	Logistic
1	5	100	10	14	14
2	10	200	23 (11. 5)	37 (18. 5)	37 (18. 5)
3	15	1000	122 (12. 2)	194 (19. 4)	194 (19. 6)
4	20	2000	251 (12. 5)	377 (18. 8)	380 (19. 0)
5	25	3000	386 (12. 8)	593 (19. 7)	593 (19. 9)
6	30	4000	514 (12. 8)	791 (19. 7)	796 (19. 9)
7	35	5000	631 (12. 6)	975 (19. 5)	987 (19. 7)
8	40	6000	757 (12. 6)	1162 (19. 3)	1169 (19. 4)
9	45	7000	861 (12. 3)	1349 (19. 2)	1360 (19. 4)
10	50	10000	1249 (12. 4)	1914 (19. 1)	1928 (19. 2)
Note: Possible error number (per 100)					

VI. IMPLICATIONS FOR INTERNAL AUDITORS

Almost all the large and listed companies have internal auditing department. The role of this department is management audit. As internal audit department must be independent from other departments, it belongs to CEO. Report of internal auditor must be addressed to CEO. If internal auditor is responsible for Cybersecurity, the incidents of attacking must be reported to CEO directly and he/she can take necessary actions immediately. Information department must be responsible for detection of attacking but they are very busy for

information processing every day. After having detected attacking, other department must take a responsibility to stop malware and reporting to a supervisor. Internal audit department can take that job.

Unfortunately, present internal auditors don't have enough knowledge and information about Cybersecurity. As a final chapter, we will give several implications for internal auditors.

- (1) Cybersecurity educational training: As we have known, incidents occurred by human error. Educational training is most effective to minimize human errors. Training courses by CYDER

and GSX are held on weekend. Personnel of internal audit department shall take educational training courses of Cybersecurity.

- (2) Daily contact with information department: Incident occurs at the information department. Internal auditors need to know what happen at the information department. With accumulated knowledge by educational training courses, internal auditors understand what happened at the information department and more important is that they should stop malwares and attacking.
- (3) Reporting and safeguarding of computer system: Report of Cybersecurity from internal audit department shall be addressed to CEO and he/she must recognize the importance and necessity of Cybersecurity. Reporting is the 1st step and CEO must proceed to safeguard computer system from attacking. This is the 2nd step. Internal auditors shall play an important role to connect the top of a company and information department.

VII. CONCLUSION

The following is the conclusion of this paper.

- (1) Educational training courses using real incidents have effects on

Cybersecurity. We used data of targeted email attacking training and Micro Hardening of GSX. Z-test results demonstrated the effects of education. 2nd session and 3rd session of targeted email attacking training and Micro Hardening are improved.

- (2) AI programs may be used for Cybersecurity to detect attacking. We made 3 prototype AI programs. Discriminant Model assumes the normal distribution and Maximum Likelihood Estimation assumes the uniform distribution. The 2 distributions were used for simplification of explanation but the simulated data is not a real distributions. This means that these 2 methods don't have a theoretical foundation. Real data is similar to the curve of Linear Logistic Regression Model.
- (3) Incident occurs at information department. It is responsible for them to detect attacking to computer system but they are busy in doing information processing. After having detected attacking and irregular information, other department must take the role to stop malware and attacking. Internal audit department can do that role. Missions of internal audit department are (a) stopping malware and recovery of computer system and (b) reporting the incidents to CEO.

ACKNOWLEDGEMENT

Mr. Takashi Suzuki, Executive Officer of GSX in Research and Development, has read the manuscript of this research paper several times from the early stage. He has given us constructive comments and advice in addition to typo. This paper has been polished by his supports. We would like to express our cordial thanks to him. Of course, 4 authors are responsible for this paper.

References

1. Aghili Shaun. Fraud Auditing Using CAATT- A manual for auditors and forensic accountants to detect organizational fraud. Auerbach. 2019.
2. Basic Act of Cybersecurity, Act No. 104, November 2014.
3. Earley, Christine, E.: Data analytics in auditing: Opportunities and challenges. Business Horizons. Vol 58. Issue 5. Pp. 493-500. 2015.
4. Information Processing Association. Information Security White Paper. 2018.
5. Jaber, Raced J. and Wadi, Mohammad A.: Auditors' usage of computer-assisted audit techniques (CAATs): Challenges and opportunities. Springer. 2018.
6. Leping, Jiang: Research on the application of computer aided audit technology. International conference on application and techniques in cyber security and intelligence ATCI 2018. pp. 921- 927.
7. Li, He. et al. Understanding usage and value of audit analytics for internal auditors: An organizational approach. International Journal of Accounting Information Systems. Vol. 28. March 2018. pp. 59- 76.
8. Ministry of Internal Affairs and Communications. Japan: Consolidated Measures for IOT Securities, 2017.
9. Ministry of Internal Affairs and Communications. Japan: WHITE PAPER, 2018.
10. National Center of Incident Readiness and Strategy for Cybersecurity (NISC): Information Security Handbook for Network Beginners. V 2. 11e. 2017.
11. National Center of Incident Readiness and Strategy for Cybersecurity (NISC): Report of the Investigation on Causes of Leakage of Japan Pension Service. 2015.
12. Waltermire Karen. et al. White Paper (DRAFT) Continuous monitoring for IT infrastructure: Techniques for auditing user activity and detecting irregular activity events within small and medium-size businesses. Computer Security Resource Center. 2019.

Critical Analysis and Improvement on Block-chain's Security and Auditing Concerns

TSE Woon Kwan Daniel;

WANG Yanbing

Abstract

Because of keen business competition nowadays, enterprises have found ways to improve efficiency of their business operations. One of the improvement tools is Financial Technology (FinTech). However, FinTech is too new that the use of it requires careful planning, implementation as well as monitoring. In this paper, the nature of FinTech is explored and then critical analysis on its security and auditing concerns. Finally, some improvements in these two concerns are provided.

Keywords: Financial technology, Distributed ledger, Block-chain, Security, Auditing.

I. Introduction

1- 1. Basics of Fintech

In today's competitive business environment, the use of good financial tools is very important for getting competitive advantages. Fintech is an abbreviation for financial technology which refers to the integration industry of financial and information technology. It also can be regarded as the low-threshold financial services carried

by the high-tech as well as Internet companies with the help of mobile Internet, big data, cloud computing, artificial intelligence and other emerging technologies. Fintech and financial products provided by bank complement to each other, rather than the subversive relationship. The nature of Fintech consists of the following two parts: First, Fintech is driven by data and technology. From the view of data dimension, the data size held by Fintech companies should be large enough.

From the view of technology dimension, new technologies are superimposed on the basis of data, which can be illustrated by Figure 1 below. Second, Fintech companies devote to provide customers with better financial service, including improving the efficiency of financial services and reducing the cost financial services (McCaffrey and Schiff 2017). The use of information technology has largely increased the amount of financial services for customers and improved the frequency of financial service, consequently, expanding the scale of

entire financial services market. The traditional financial institutions may be adversely affected by the new financial technology companies. The greatest impact of Fintech is the satisfaction of the financial requests which cannot be met in the past. In a word, Fintech just reduce the threshold of financial services so that inclusive finance will become possible to be implemented. Fintech companies are committed to providing personalized services to customers.

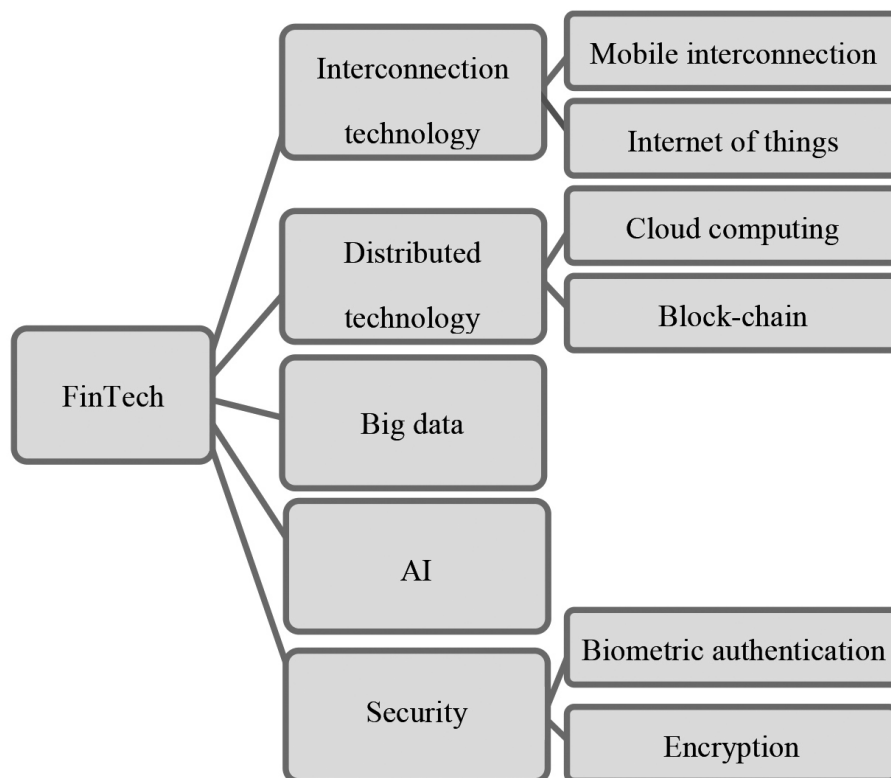


Figure 1: The components of Fintech

The core of financial products is risk pricing. Under the current financial service conditions, meeting the needs of customized financial service is difficult to be realized,

since it will consume much money. However, Fintech can effectively solve the problem. For example, when providing loans, loan interest rates for personal are different, according to the

credit data analysis. When choosing the most appropriate portfolio according to personal financial goals and risk attributes, all Fintech services only need clicking mouse to complete (Wiegner 2016). Based on characteristics of Internet users, more innovative financial products are born.

1- 2. Distributed Ledger

Distributed ledger is widely regarded as the representative technology with great potential, also most likely to have a major or even subversive impact on the current financial business model (Maull et al., 2017). The technical principle of distributed ledger is all users in a network record any transaction information synchronously, verify the authentication of information mutually, rather than depending on traditional intermediary, including stock exchange, banks. By mutual verification between users, reduce the possibility of some information being forged, modified by a few users and enhance the direct trust between both transaction parties, so as to greatly reduce the cost of intermediary.

1- 3. The Role of Block-chain Technology in FinTech

Among all technologies involved in distributed ledger, block-chain is the most important and representative technology. The general process can be illustrated as follows: When a transaction occurs, the transaction participants can submit the transaction information to the network. Then

the transaction information is encrypted and becomes unmodified, existing as a packet form named as block. Each block needs to be sent to other participants in the network, in order to synchronously compare and verify the history information recorded by these participants' distributed ledgers (Maull et al., 2017). Only the vast majority of participants have recognized the authenticity and validity of the block. It can then be stored in the distributed ledger of each participant and make as a chain with previous blocks which form the block-chain.

In short, the block-chain characteristics can be summarized as follows: (1) Decentralization: The center of the management mechanism does not exist in the network, but a distributed point to point network structure, each point in the network equivalent access authority; (2) Autonomy: All points can be free to exchange data based on the consensus specification and protocol among a de-trust environment; (3) Security: Using asymmetric cryptography technology to encrypt transaction data, at the same time guaranteeing transaction data is theoretically difficult to be modified with the help of Proof of Work mechanism; (4) Transparency: all transactions recorded in the whole network is open and transparent, which solve the problem on asymmetric information (Romano 2017).

II. Critical Analysis on Security and Auditing Aspects

Block-chain is like a sword with two sides. Besides having many benefits and advantages, its implementation also has some risks and disadvantages. Lamberti (2017) discussed that using block-chain technology has the disadvantages including: (1) Throughput: Block-chain exchange for system security at the expense of its performance; (2) Concurrent process: Block-chain cannot support access of high concurrent client; (3) Access control: How to design decentralized access control for block-chain is also a problem to be solved; (4) Query statistics: Block-chain is inconvenient to inquire in Non-Key and history data; (5) Expansibility: Most of the block-chain platform overall performance declined with the increase of the number; and (6) Transaction processing: Block-chain platform mainly rely on the underlying database to provide transaction processing, while the underlying database is mostly Key-Value database without transaction processing capabilities. The following paragraphs focus on three important areas for critical analysis:

2-1. Robustness

The robustness of the block-chain payment is mainly related to its security performance. How secure the block-chain payment is, can be regarded as the fundamental factors for its application and development. For payment process, data security and transaction

information security always deserve much attention. First, the block-chain technology has the decentralization characteristic which can highly improve its security performance in data protection, compared with other centralized system. The whole network has no centralized hardware or management system and each participant point can get a copy of the whole database. The damage of any point will not affect the whole system operation. Therefore, the possibility of hacking into the block-chain system is almost zero. The modification of the database on a single point is invalid, which means it cannot affect the data content on other points. Thus, the more points participate in the system, the higher the data security will be.

Second, ensuring the asset ownership in payment process is the security foundation of digital asset protection. Block-chain provides the ownership authentication function based on the standard digital signature algorithm and is considered as an effective way to protect digital assets. In the block-chain, each payment is stored in the block transaction record which contains the transaction content and the public key certification of the asset receiver. Compared with the common public key certification, it removes the public key owner identity information, thus ensuring the anonymity of the asset receiver. The asset receiver only needs to keep the private key corresponding to the public key so that the ownership of the asset can be declared and verified.

The asset ownership proof in block-chain

payment is divided into two processes: One process is making payment signature. Three parts are bound together by the asset payer, including the hash value of the asset receiving record for last time, payment information for this time and public key certification of asset receiver. Then the asset payer uses its own private key to make digital signature. The digital signature indicates that the payment is authorized by the asset payer. Another process is verifying payment. For a valid payment signature, anyone can verify the payment signature based on the payer's public key certification stored in the previous payment block. However, this process does not need to disclose the identity of the user.

Signature technology is also the basic guarantee to ensure block-chain payment security. Some new signature techniques have been introduced into block-chain construction, such as blind signature, group signature, ring signature, aggregation signature, threshold signature, etc. The introduction of these signature technologies can meet demands of payment process. Compared with the traditional digital signature technology, these advanced signature techniques have special security attributes and are usually provably secure. In addition, providing higher security and better performance is conducive to improve the application effect of block-chain in payment.

2- 2. Flexibility

The application of block-chain technology

in payment system brings a lot of flexible and convenient changes. This part explains the flexibility of block-chain payment in an object-oriented way (Eikmanns & Sandner 2015). First, based on practical application, block-chain payment can effectively solve the complex problems of international cross-border payment. Secondly, from the technical point of view, the block-chain technology is applied to the cryptocurrency payment system, which can effectively overcome the long-standing problem of double payment for cryptocurrencies. The following will start from this two aspects, specifically analyze how block-chain payment optimize the process, and solve the problem.

For the first aspect, it is the international cross-border payment. There are some prominent business bottlenecks in the existing cross-border payment process. First, the transaction chain is long, the participants are more, and the intermediate links produce considerable expenses. Second, the operation is not convenient, such as payment can be conducted only in the banking hours, the account number and payment path code must be accurately entered. Third, the settlement process is very slow, often takes a couple of days. For a long time, banks and clearing institutions are trying to achieve the following ideal state, including reducing transfer costs, improving cross-border payment security and speeding up settlement process.

The block-chain technology can provide solutions to these problems. A unified

distributed ledgers system verifies payment through consensus mechanism through each participant nodes. It doesn't need any trust centers. Banks can pay point to point without the help of third parties. This can save many intermediaries and links, to achieve real-time arrival, which can meet the cross-border payment timeliness and convenience requirements. Currently a relatively feasible landing scheme is primarily using block-chain payment within a bank group, generating private chain for cross-border payment process, to realize the synchronous management of money and account, and to avoid the reconciliation between different databases. When multiple banking groups have the practical basis of block-chain payment, the establishment of interbank block-chain payment system is workable. At the same time, from the supervisor's point of view, all payment information recorded by block-chain cannot be tampered. All supervisors and auditors have access to the block-chain.

For the second aspect, it is the double payment problem. The so-called "double payment", refers to that cryptocurrencies, no matter how strictly they are encrypted, are always a string of binary code, which can be easily copied, because of the infinite replicability of cryptocurrencies, if there is no center institutions, there is no way to confirm whether a cryptocurrency has been spent. Therefore, in a payment process, there must be a credit third party to retain payment record, so as to ensure that each cryptocurrency will only

be spent once.

So, whether it is a centralized system or a centralized system, to solve the double payment, the consensus mechanism for each transaction must be conducted. With the help of combination of timestamp and consensus mechanism, block-chain payment can effectively solve the problem. Every block is labeled with a timestamp and published among the whole network, to ensure that every cryptocurrency can't be paid again after first payment. If and only if all payments contained in the block are valid and never existed before, then every participant node agrees with the validity of the block.

2- 3. Auditability

The auditability of block-chain payment is mainly attributed to the unique natures of block-chain technology, including data transparency, non-tampering and traceability. This part will explain the auditability of block-chain payment through the analysis of the above three natures. What's more, the control for audit purpose used by block-chain payment will also be described in this part.

The block-chain, which is actually a database, can be seemed as the transaction log. Each successfully approved payment would be recorded in a block, and then the block would be linked into the chain. Frankly speaking, the block-chain itself is the basic trail for auditing (Wei 2016). The natures brought by its operation mechanism play the important roles in improving audit control.

The first nature to be introduced is data transparency. The information of each payment is transparent and open to all nodes, which is the basis for the payment system to maintain the trust of the whole network node. With high transparency, data recording and processing can be restored by all nodes. In this mode, every node can act as the auditor to review each payment conducted in the network.

Another two natures, non-tampering and traceability, are critical factors for the auditability of block-chain payment, which are both based on the application of timestamp technology in its data storage structure. So it is necessary to make a simple introduction about the timestamp technology. Timestamp technology is not a new technology, but it is a great innovation to apply it to block-chain technology. The timestamp is the time when the current block data is written and is stamped when the block is created. Its existence provides the trace evidence for each payment. Each participant node in the network can record the payment generating time into block by using timestamp. Once the payment is approved by most of participant node, the block would link to block-chain following the time sequence. This mechanism makes the audit tracing process convenient. And theoretically speaking, generating fabricated record is almost impossible to accomplish. Besides, once the block linked in the block-chain, the payment information is permanently stored, which means no change is allowed. This mechanism can prevent any malicious tampering, which

effectively increases the accuracy of audit process.

Totally speaking, the application of timestamp helps the block-chain to form a database that cannot be tampered or fabricated. The block-chain links the blocks labeled with timestamp following time sequence, and integrates the time dimension into the block-chain skillfully. Tamper resistant and temporal dimension gives the characteristics of traceability and security, which high improves the auditability of block-chain payment. From the control standpoint, the nature of traceability makes great contribution in audit trail control. While the nature of non-tampering makes great contribution in database control (Masry & Reck 2008).

III. Suggested Improvement on Block-chain Security and Auditing Aspects

The payment application based on block-chain is known for its security. The non-modifiability and transparency of the distributed ledger technology make it an ideal choice for maintaining transaction record integrity. Although the use of block-chain in payment is becoming more and more mature, there is still room for further improvement which can be realized by biometric technology. The combination of biometric technology and block-chain technology should be able to enhance the security of payment process.

The core issue of payment front end is

identity authentication. In general, the problem of authentication can be summarized as: how to prove the "I am I"; "you are you"; how to confirm that the sending part is indeed the owner of account. That is to say, if "I am I" is successfully identified, my transaction is undeniable. This point plays a real important role in the development of block-chain payment. According to the whole logistic flow, security rules are used to confirm the authenticity of each transaction. Authenticity of the transaction ensures the authenticity of the circulation of funds. All authenticity guarantees the legality of the balance in account.

(Oscar et al., 2019) describes how the combination of biometrics and block-chain can significantly reduce the risk of fraud in the payment industry and comply with the existing regulatory framework. In the article, the authors point out any people who can access to other people's mobile phone or e-mail can easily approve payment (cost other people's money) using the same or different devices. Biometric technology can almost eliminate the possibility that fraudsters pretend to be account owner and approve transactions.

Next, the feasibility for biometric technology used in block-chain payment will be analyzed. For some public chain such as bitcoin, the user's identity does not need to be verified. Only by digital signature to ensure that the user has a private key, then the user can do related operations. Even non-authentication can be regarded as one of the ways in which bitcoin, Ethernet and other virtual currencies

are used to increase anonymity. However, this method can also bring some other problems, such as poor experience feeling. A long string of irregular combination of digital letters is quite inconvenient to remember. Once the private key is lost or forgotten, it cannot be retrieved. But it is obvious that most of the users are not able to accept the fact that their assets will not belong to them if they lost their private key.

For financial sector, authentication not only involves the experience feeling but also satisfies the legitimacy conditions. According to information security laws and regulations in some countries, the private key of core financial institutions must be contained in a physical medium which is independent to node equipment (like U shield). That is to say, the physical device which contains the private key can represent identity. This experience seems to be enough to meet user needs in the financial field but for ordinary users is still not perfect. People are used to the account password in the system. Furthermore, today users gradually prefer to the mobile phone terminal, so the experience feeling will be very bad if users still need a physical media to finish the signature process.

Biometric is considered to be one of the best solutions for block-chain technology, to solve the problem existing in user identity authentication. Biometric technology can use physical characteristics or behavioral characteristics inherent in the human body to verify people's identity. The generally

used biological characteristics include face, iris, fingerprint, palm print, voice. Now more commonly used fingerprint, for example now people need to enter the fingerprint when applying ID card. There is no doubt that with technical support fingerprints are easy to link reality identity and online data on policy.

In our research, there are two constructive solutions on how the biometric fingerprint verification is applied to block-chain payment. The first solution is to introduce the double insurance mechanisms. That is to say, user is required to verify fingerprint before accessing the account and making encryption using the private key which aims to confirm that user is indeed the account owner. In addition to the combination of fingerprint and private key, no other method can transfer asset in the account. In other words, it is possible that other people can acquire the private key but almost not possible for fingerprint. Actually this solution mainly focuses on improving payment security but do nothing to improve the user experience.

Another solution is the evolutionary version of the first solution. According to the first solution, account owners have to keep their private keys by themselves. But generally speaking, a long string of irregular combination of digital letters is really easier to be forgotten, which means asset in the corresponding account is lost at the same time. This is undoubtedly that the ownership of asset is greatly threatened. In the second solution, we envisage that a mapping relation can be conducted by system between fingerprint

and private key. Simply speaking, the private key can be kept by system. Once fingerprint authentication finishes successfully, account owner does not need use private key to encrypt any more. However, this solution involves the private key storage process which needs more effective protection measures to make sure the private key cannot be stolen by hackers. The detailed contents will be elaborated in our future research.

Although block-chain technology is not a tool for auditing, it would have the impact to the traditional auditing technique that affect auditing and assurance profession. Although there are a couple of non-proven services provided by some consultancy companies in handling such impact on auditing, their approaches and methodologies are proprietary and confidential that there is no way to trace their success. In fact, the ultimate goals of auditor's work are to detect any possible material misstatement in the accounting records as well as checking whether the internal controls exist and working reliably supported by evidences. AICPA (2017) asserted that an audit involves an assessment that recorded transactions are supported by evidence that is relevant, reliable, objective, accurate and verifiable. Therefore, the acceptance of a transaction into a reliable block-chain may constitute sufficient appropriate audit evidence for certain financial statement assertions. For example, in smart-contract block-chain application, management is responsible for establishing controls to verify whether the

smart-contract source code is consistent with the intended business logic. In other words, although it is not so urgent for auditors to be competent in handling block-chain technology, they need to monitor the developments in block-chain technology because it will impact their clients' information technology systems.

IV. Conclusion

In summary, Fintech is one of critical success factors in today's business world. Block-chain is the core technology in Fintech but it is not almighty as discussed above. Thus, Fintech's potential security and auditing problems are the barriers for successful implementation. Some other tools have to be used in tandem with Fintech. One of these is biometric technology. Assistance of biometric technology is not the necessary condition for improving block-chain payment. Without biometric technology, block-chain payment can still be implemented. If block-chain payment intends to be popularized in people's real life, law regulation and user experience are the two problems which must to be solved. Biometric is one of the possible solutions for the two problems. Simply speaking, biometric technology is likely to be a bridge which is able to lead block-chain payment to real life. Last but not least, block-chain's security and auditing concerns do have impact to auditor's profession. Auditors are no need to be fear about the complexities of its technology but they should get sufficient acquaintance with its

technology in order to prepare for the changing auditing requirements and standards.

References

1. AICPA and CPA Canada, 2017, Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession, Deloitte Development LLC.
2. Eikmanns, B., Sandner, P. , 2015, Bitcoin: The Next Revolution in International Payment Processing? An Empirical Analysis of Potential Use Cases. SSRN Electronic Journal.
3. Lamberti, F., Gatteschi, V., Demartini, C., Pranteda, C., & Santamaria, V. , 2017,Blockchain or not blockchain, that is the question of the insurance and other sectors. IT Professional.
4. Masry. E., Reck, J.L. , 2008, Continuous Online Auditing as a Response to the Sarbanes-Oxley Act. Managerial Auditing Journal, 23(8), pp. 779- 802.
5. Maull, R., Godsiff, P., Mulligan, C., Brown, A. and Kewell, B. , 2017, Distributed ledger technology: Applications and implications. Strategic Change, 26(5), pp. 481- 489.
6. McCaffrey, M. and Schiff, A. , 2017,Finclusion to Fintech: Fintech Product Development for Low-Income Markets. SSRN Electronic Journal.
7. Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana, Ruben Vera-Rodriguez , 2019, Blockchain and Biometrics: A First

- Look into Opportunities and Challenges,
<https://arxiv.org/abs/1903.05496>
8. Romano, D and Schmid, G. , 2017, Beyond the Bitcoin: A Critical Look at the Block-chain-Based Systems. Cryptography, p. 15.
 9. Wei, Z. , 2016, Application Prospect of Block-chain Technology in Accounting. Friend of Accounting, 17, pp. 122- 125.
 10. Wiegner, B. , 2016, Financial Management for Innovation Fintech-Start-Ups vs. Usual Companies. SSRN Electronic Journal.

銀行業重大裁罰案件思考建置數位證據 鑑識標準

Discussion Establishment of Digital Evidence Forensic Standard Operation Procedure in Banking Major Enforcement

林宜隆 I-Long Lin

元培醫事科技大學資訊管理系教授

電腦稽核協會理事長暨舞弊稽核與數位鑑識委員會主任委員(2012~2016)

cyberpaul747@gmail.com

楊慧茹 Hui-Ju Yang

宜蘭大學數位學習碩士在職專班

ahl123@ms45.hinet.net

摘 要

銀行是經濟中最為重要的金融機構之一。近年來，國際間陸續發生多起重大金融事件，如 2016 年 7 月：第一銀行 ATM 盜領案，駭客以一銀倫敦分行的電話錄音系統作為跳板，最終遙控了全臺灣 41 臺一銀 ATM，盜走 8,327 萬餘元，2016 年 9 月：第一銀行及第一金證券遭駭客進行分散式阻斷服務攻擊 (DDoS)，個人網銀、企金網銀、證券商電子下單平臺的服務分別中斷數小時，2017 年 10 月：駭客入侵遠東銀行的國際匯款交易系統 (SWIFT)，產生營運缺失而影響整體業務經營，也影響國民經濟與生活，金融監督管理委員會 (以下簡稱金管會) 以健全金融機構業務經營，維持金融穩定與促進金融市場發展。

本文依照國內學者林宜隆教授 (2015) 等的研究方法繼續分析國內近年來的銀行裁罰案件，採用內容分析法之研究方法，分類彙整營運作業的內部稽核缺失及其影

響的內部控制目標，擬定不同營運作業的關鍵性查核項目及銀行業內部稽核流程之設置建議。

關鍵詞：裁罰案件、資安治理、舞弊稽核、鑑識會計、數位證據鑑識標準。

Abstract

Banks are one of the most important financial institutions in the economy. In recent years, there have been many major financial events in the international community. For example, in July 2016: the first bank ATM piracy case, the hacker used the telephone recording system of a silver London branch as a springboard, and finally remotely controlled 41 Taiwanese silver. ATM, stealing more than 83.27 million yuan, September 2016: First Bank and First Gold Securities were hacked to conduct Decentralized Blocking Service Attack (DDoS), personal online banking, corporate gold online banking, securities firm electronic order platform The service was interrupted for several hours, October 2017: The hacker invaded the Far East Bank's International Remittance Trading System (SWIFT), which caused a lack of operations and affected the overall business operations, as well as the national economy and life. The Financial Supervisory Commission (hereinafter referred to as the Financial Management Association) To improve financial stability and promote the development of financial markets by improving the business operations of financial institutions.

In accordance with the research methods of domestic scholar Lin Yilong (2015), this paper continues to analyze domestic bank penalties in recent years, adopts the content analysis method, and classifies the internal auditing errors of operational operations and the internal control objectives of their impacts. Key auditing of operational operations and recommendations for setting up the internal audit process of the banking industry.

Keywords : Major Enforcement, Information security governance, Forensic accounting, Fraud, Digital Evidence Forensic Standard Operation Procedure

壹、緒論

民國 103 年某銀行因為離職員工將客戶個人資料下載之私人外接儲存裝置，經金管會核定未妥適建立內部控制制度，依違反銀

行法核處新台幣 300 萬元罰鍰，本新聞事件再次凸顯保護客戶資料的重要性；民國 105 年 7 月 11 日，國內金融史上首件 ATM 盜領案，第一銀行 20 家分行、51 台 ATM，7 月 9 日至 11 日，遭多名外籍人士盜領新臺

幣 83,277,600 元；民國 106 年遠東銀行遭駭盜轉 18 億元案發至今，雖然超過 9 成 9 的款項都已追回，但對企業 IT 部門、銀行 CIO 或資安圈而言，更重要的是找出駭客入侵銀行的手法。因此銀行不管是面對一般業務或者金融商品的經營，均應訂控管流程及標準，而控管是否能夠落實，就端賴於內部稽核功能的有效發揮。

本文擬從金管會銀行局在 103 年 1 月至 107 年 6 月所公佈的裁罰案件中，由案件所違反內部控制法令的事實進行內部稽核缺失的探討，以達到以下之研究目的：

1. 分類彙整裁罰案件產生內部稽核缺失金額。
2. 分析彙整內部稽核人員在查核營運作業項目產生的稽核缺失，並提出關鍵性查核項目，作為執行查核時之應注意事項。
3. 建議數位證據鑑識標準作業程序設置。

貳、文獻探討

一、內部稽核與內控控制

(一) 內部稽核的定義及目的

內部稽核足以顯示在企業組織的營運中扮演不可或缺的角色，也是組織是否落實風險之重要依據，因為內部稽核是內部控制下重要的監督要素，然而為了確保內部控制能有效實施，持續性稽核則是組織達到持續性監督的不二法門，因此企業組織須將內部稽核依其所具備的意義，獨立位

階在董事會下，以達到經營權與所有權隔離但不脫離的前提，可獨立行使監督與稽核權（連煥明 2003）。

(二) 內部控制的意義及目標

內部控制能幫助組織達成其績效及營利目標，預防資源的損失，保證其財務報導可靠性、遵循相關法令，避免組織的名聲受損及其他後果；且良好的內部控制所包含的檢查與覆核，可以保障組織免於因人為缺失所造成之損失。

(三) 國內金融業內控內稽之法令依據

法令規範都顯示了政府要求金融業能先達到自我管理控制及自律稽核的目的。依照民國 107 年 03 月 31 日本國「金融控股公司及銀行業內部控制及稽核制度實施辦法」第一章第四條所規定：

內部控制之基本目的在於促進金融控股公司及銀行業健全經營，並應由其董（理）事會、管理階層及所有從業人員共同遵行，以合理確保達成下列目標：

1. 營運之效果及效率。
2. 報導具可靠性、及時性、透明性及符合相關規範。
3. 相關法令規章之遵循。

第一款所稱營運之效果及效率目標，包括獲利、績效及保障資產安全等目標。

第二款所稱之報導，包括金融控股公司及銀行業內部與外部財務報導及非財務報導。其中外部財

務報導之目標，包括確保對外之財務報表係依照一般公認會計原則編製，交易經適當核准等目標。

(四) 金融業之營運作業項目

根據我國「金融控股公司及銀行

業內部控制及稽核制度實施辦法」第8條規定，內部控制制度應涵蓋所有營運活動，並整理營運活動演變，如表1。

表 1 金融業之營運作業項目演變

修正日期	業務規範
民國 99 年 03 月 29 日	(一)投資準則。 (二)客戶資料保密。 (三)利害關係人交易規範。 (四)股權管理。 (五)會計暨財務報表編製流程、總務、資訊、人事管理(銀行業應含輪調及休假規定)。 (六)對外資訊揭露作業管理。 (七)金融檢查報告之管理。 (八)其他業務之規範及作業程序。 金融控股公司業務規範及處理手冊應另包括子公司之管理及共同行銷管理。 銀行業務規範及處理手冊應另包括出納、存款、匯兌、授信、外匯、新種金融商品及委外作業管理。
民國 101 年 03 月 02 日	(一)投資準則。 (二)客戶資料保密。 (三)利害關係人交易規範。 (四)股權管理。 (五)適用國際會計準則之管理、會計暨財務報表編製流程、總務、資訊、人事管理(銀行業應含輪調及休假規定)。 (六)對外資訊揭露作業管理。 (七)金融檢查報告之管理。 (八)金融消費者保護之管理。 (九)其他業務之規範及作業程序。 金融控股公司業務規範及處理手冊應另包括子公司之管理及共同行銷管理。 銀行業務規範及處理手冊應另包括出納、存款、匯兌、授信、外匯、新種金融商品及委外作業管理。
民國 103 年 08 月 08 日	(一)投資準則。 (二)客戶資料保密。 (三)利害關係人交易規範。 (四)股權管理。 (五)適用國際會計準則之管理、會計暨財務報表編製流程、總務、資訊、人事管理(銀行業應含輪調及休假規定)。 (六)對外資訊揭露作業管理。 (七)金融檢查報告之管理。 (八)金融消費者保護之管理。 (九)其他業務之規範及作業程序。 金融控股公司業務規範及處理手冊應另包括子公司之管理及共同行銷管理。 銀行業務規範及處理手冊應另包括出納、存款、匯兌、授信、外匯、新種金融商品及委外作業管理。

<p>民國 104 年 05 月 12 日 民國 105 年 07 月 05 日</p>	<p>(一)投資準則。 (二)客戶資料保密。 (三)利害關係人交易規範。 (四)股權管理。 (五)財務報表編製流程之管理，包括適用國際財務報導準則之管理、會計專業判斷程序、會計政策與估計變動之流程等。 (六)總務、資訊、人事管理（銀行業應含輪調及休假規定）。 (七)對外資訊揭露作業管理。 (八)金融檢查報告之管理。 (九)金融消費者保護之管理。 (十)其他業務之規範及作業程序。 金融控股公司業務規範及處理手冊應另包括子公司之管理及共同行銷管理。 銀行業務規範及處理手冊應另包括出納、存款、匯兌、授信、外匯、新種金融商品及委外作業管理。</p>
<p>民國 106 年 03 月 22 日 民國 107 年 03 月 31 日</p>	<p>(一)投資準則。 (二)客戶資料保密。 (三)利害關係人交易規範。 (四)股權管理。 (五)財務報表編製流程之管理，包括適用國際財務報導準則之管理、會計專業判斷程序、會計政策與估計變動之流程等。 (六)總務、資訊、人事管理（銀行業應含輪調及休假規定）。 (七)對外資訊揭露作業管理。 (八)金融檢查報告之管理。 (九)金融消費者保護之管理。 (十)重大偶發事件之處理機制。 (十一)防制洗錢及打擊資恐機制及相關法令之遵循管理，包括辨識、衡量、監控洗錢及資恐風險之管理機制。 (十二)其他業務之規範及作業程序。 金融控股公司業務規範及處理手冊應另包括子公司之管理及共同行銷管理。 銀行業務規範及處理手冊應另包括出納、存款、匯兌、授信、外匯、新種金融商品及委外作業管理。</p>

二、ISO/IEC 27014: 2013 資安治理

國際標準組織 (International Organization for Standardization, ISO) 針對資安治理規

範，資安治理範圍包含資安治理本身，以及涉及資安治理的資訊技術部分，其上受組織治理的監督、影響。如圖 1。

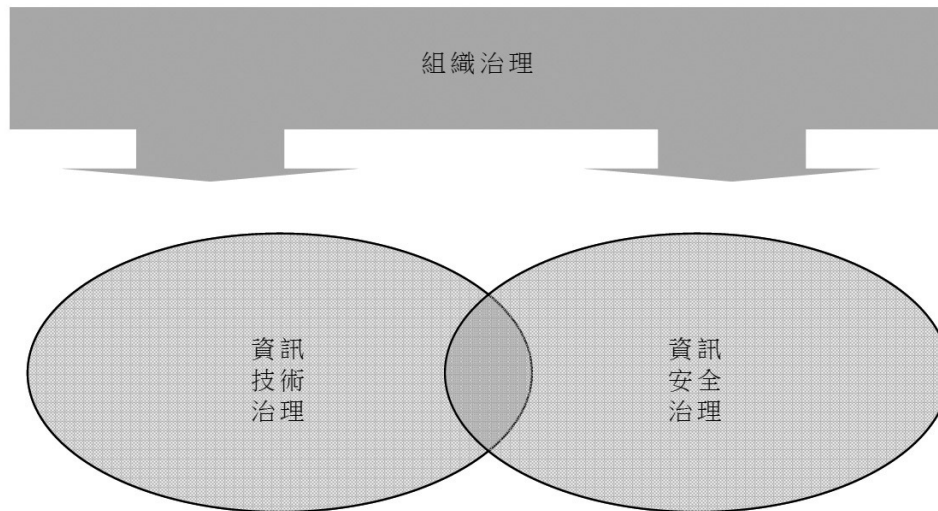


圖 1 資安治理與資訊技術治理間之關係

資安治理規範，治理單位以 EDM(評估 (Evaluate)、指導 (Direct)、監視 (Monitor)) 方式形成治理過程，向下監督、管理資訊安全管理執行單位，並由治理單位向上進行溝

通，回應組織利害關係人之要求，且整個運作機制對外可以由獨立機構提供客觀意見。如圖 2。

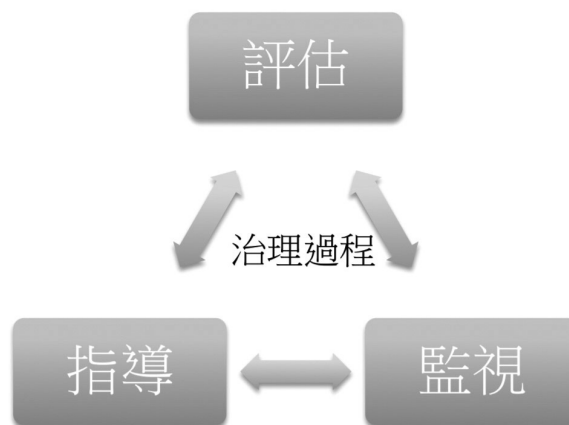


圖 2 治理過程

治理單位履行”評估”、”指導”、”監視”及”溝通”過程，以治理資訊安全。

此外，”保證”過程提供關於資安治理及

達到之等級的獨立及客觀意見。

如表 2，資安治理過程定義、治理單位和執行管理單位採取的作為。

表 2 資安治理過程定義及採取的作為

過程	定義	治理單位宜採行的作為	執行管理單位宜採行的作為
評估為治理過程	依據目前過程及所規畫變更，考量目前及預測安全目標達成情形，並決定是否須調整已達成未來策略目標之最佳化。	1. 確保營運計畫自始即將資訊安全議題納入考量 2. 因應資訊安全績效結果，啟動必要行動並排優先順序	1. 確保資訊安全適切支援並維持營運目標 2. 提交具重大衝擊之新資訊安全專案與治理單位
指導為治理過程	指出關於需實作之資訊安全目標及策略方向。 包括：資源之等級變更、資源配置、活動之優先序，以及政策、重大風險接受及風險管理計畫之核准	1. 決定組織風險胃納 2. 核准資訊安全策略及政策 3. 配置適當投資及資源	1. 發展及實作資訊安全策略及政策 2. 對其資訊安全目標與營運目標 3. 宣導正面的資訊安全文化
監視為治理過程	治理單位能評鑑策略目標達成情形	1. 評鑑資訊安全管理活動之有效性 2. 確保符合內部及外部要求事項 3. 考量變動之營運、法律及法規環境及其對資訊風險的潛在衝擊	1. 對營運前景中選擇適當績效度量 2. 對治理單位提供資訊安全績效結果之回饋，包括治理單位先前確定之決議執行績效及其對組織之衝擊 3. 對治理單位警示影響資訊風險及資訊安全之新發展
溝通為雙向治理過程	治理單位藉以與利害相關者交換關於適切於其特定需求之資訊安全的資訊	1. 向外部利害相關者報告組織實行相稱於其營運性質的資訊安全等級 2. 通知執行管理階層以識別資訊安全議題的所有外部審查結果，以及要求矯正措施 3. 辨識與資訊安全有關之法規義務、利害相關者期望以及營運需求	1. 對治理單位，建議其所有須注意及可能須決策之事項 2. 對相關之利害相關者，只是支援治理單位之指立即決策，須採取之動作細節
保證為治理過程	治理單位藉以委任獨立及客觀稽核、審查或驗證。將識別及驗核，為達所期望之資訊安全等級，與施行治理活動及進行運作相關之目標及行動。	對其如何遵循所期望資訊安全等級之可歸責性，委任獨立及客觀的專家意見	支援由治理單位所委任之稽核、審查或驗證

三、舞弊稽核

舞弊是有意或故意欺騙他人，而導致善意的一方遭受損失或意圖不軌之人獲得利益。美國會計師協會查核準則第 99 號公報：財務報表查核舞弊之考量 (SAS No. 99: consideration of fraud in a financial statement audit)，定義舞弊發生的三大要件：誘因或壓力、機會、態度，且合理化其舞弊行為。舞弊的發生歷程有三，亦可說為事

前、事中、事後三個階段，分別就我國審計準則公報第 43 號、美國審計準則公報第 99 號、坊間書籍，有關舞弊的預防、偵測、調查、回應，防制的方法概述如下：

按舞弊的發展過程，可區分為防制、稽查、鑑識調查等三個歷程，如圖 3，防弊措施可分為預防、偵測、調查、回應等四個階段。



圖 3 舞弊三歷程

(一) 舞弊三角理論與犯罪 MOP 理論

1. 舞弊三角理論 (Fraud triangle)

舞弊三角理論係 Donald R. Cressey 在 1950 年訪談約 200 位舞弊者，所提出的研究假說，指出職場產生舞弊的三項

本質因素為：機會、誘因或壓力和態度或合理化行為解釋，三者交互影響，亦即為審計準則第 43 號公報第 12 條所述，造成舞弊發生的因素。如圖 4。

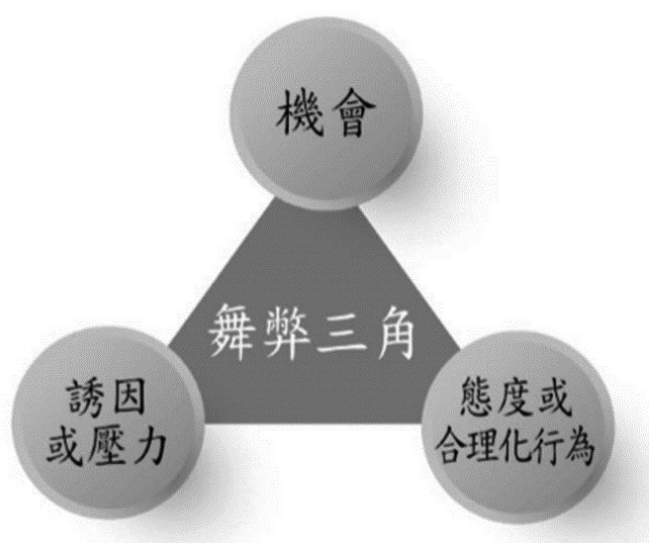


圖 4 舞弊三角理論圖

機會 (Opportunities)

若是缺乏有效的內部監管，員工的職權可提供犯罪的機會，尤其是負責處理重要文件，或經常接觸私隱資料的職位，如醫護或財務機構的職員等。未經許可出售個人資料圖利已是常有的事。

誘因或壓力 (Incentive/pressure)

壓力是指個人面對的內在或外在壓力，尤其是一些難以解決的財政困難，但不一定是經濟環境造成。壓力也可能來自朋輩、家庭或社會期望。最常見的就是急於成家置業、因嗜賭而欠債，甚至是急欲籌集資金趁牛市買股票等，因而形成巨大的心理和經濟壓力。

態度或合理化行為 (Rationalization)

Cressey 指出許多犯事者都不認為自己是罪犯，只是運氣不好而碰巧遭逮著罷了。他們也會自圓其說，相信自己的罪行是合理的。

四、鑑識會計

(一) 鑑識會計的定義與功能

何謂「鑑識會計 (Forensic accounting)」？「Forensic」一字，根據美國傳統字典《The American Heritage Dictionary》係指「屬於或使用於法律訴訟程序或正式爭論」(Of or used in legal proceedings or formal debate)；而牛津英文字典《Oxford English Dictionary》，「Forensic」乃指「與法庭有關，或在法庭中使用；適合或可用於法庭中的答辯。」另大陸簡明英漢辭典「Forensic」是指「法庭的，適合於辯論的」，我國則稱 Forensic 為「鑑識」，張熙懷檢察官指稱為有鑑識職責之人，回溯過去，或進行相關的檢視，以探究真偽。將鑑識運用到法律上的紛爭，即屬「鑑識會計」。鑑識會計即是在為法庭或其他與法律有關之目的下，所執行的會計專業工作。(林宜隆、楊期荔 2011)，鑑識會計的定義及功能，如表 3、表 4。

表 3 鑑識會計的定義

機構 / 學者	定義
美國會計師協會 (AICPA)	鑑識會計是應用會計原則、會計理論、會計訓練等各種會計知識到一法律紛爭上之事實問題及假設問題。
Bologna and Lindquist	鑑識會計是一項在證據法 (Rules of evidence) 的範圍內，將財務會計上的知識以及調查性之心態應用到未解決之議題上。

表 4 鑑識會計的功能

功能	鑑定人	說明	服務項目
調查性會計	由公司委任	鑑識會計人員著重的重心，在於針對犯罪動機、機會或其可獲取之利益等蒐集相關證據。	主要為財務報表詐欺、舞弊偵查等。
訴訟支援	由法庭委任	任何非律師者在訴訟過程中，對律師所提供之專業協助。	擔任專家證人 (Expert witness)

1. 調查性會計 (Investigative accounting)

鑑識會計人員通常會涉及非常廣泛的調查活動。調查性會計通常都與犯罪的調查相關。在調查性會計中，鑑識會計人員著重的重心，在於針對犯罪動機、機會或其可獲取之利益等蒐集相關證據 (Bologna and Lindquist 1995)。一般而言，社會大眾對調查性會計運用的場合，多聯想到白領階級的商業犯罪 (White-Collar Crime, WCC)。包括了基層員工可能涉及的員工偷竊 (Embezzlements) 或詐欺事件，例如將收到之現金款項予以挪用、偷竊公司之資產等行為；高階經理人員可能涉及的犯罪行為，主要為財務報表詐欺等。

鑑識會計在其發展的初期，在偵查舞弊上多屬被動 (Reactive) 的型態。在舞弊的偵查過程中，首先由舞弊檢查人員 (Fraud examiners) 或者舞弊查核人員 (Fraud

auditors) 主動偵查可能的舞弊。在上述人員發現舞弊之證據後，再由鑑識會計人員來進行後續的工作。另外，鑑識會計為會計專業人員所提供的服務；而舞弊調查則僅針對舞弊事件進行調查，且執行者也不一定必須非為會計專業人員不可 (Wells 2003)。然隨著鑑識會計近年來的發展，其所能提供的服務涵蓋的範圍也越來越廣。鑑識會計在偵查舞弊上的角色，從原先的被動型態轉變為也包括了主動的偵查舞弊之功能 (陳紫雲、C Pacini 2006)。亦即就今日的鑑識會計的內容與型態而言，已經包括了所謂的舞弊偵查 (陳虹任 2006)。

2. 訴訟支援 (Litigation support)

AICPA 認為，所謂的訴訟支援就是「任何非律師者在訴訟過程中，對律師所提供之專業協助」 (Wagner and Frank 1986)。訴訟支援主要是鑑識會計人員作為調查案件中，在法律之爭議或者是財務補償之要

求等議題中，提供其專家之意見。在訴訟中，鑑識會計人員檢視個人或公司之帳冊以及相關紀錄等，以協助律師準備其手中之案件。

鑑識會計人員最常遇到的情況，就是對經濟損失之量化與分析。最典型的訴訟支援之委任，就是計算由於違反契約所造成之財務損失。其中可能必須衡量收益與利潤之損失，同時也有可能需要對企業之財產或業主權益等進行評價。在訴訟支援中使用鑑識會計的範圍可以十分廣泛，雖然一般都認為只有在進入審判的階段才會使用到鑑識會計，但事實上鑑識會計也可應用在審判前之支援，例如撰寫報告、確立因果關係、蒐集真相、翻譯術語等。同時，雇用鑑識會計人員者，有可能是在法庭中的任何一方，甚至包括法庭本身（如法官）。

此外，鑑識會計在訴訟支援中，另外一項十分重要的功能，即擔任專家證人（Expert witness）。一般的情況下，證人是不允許在作證的過程中陳述其意、或者是結論等。

亦即，證人僅能就其感官知覺（視覺、聽覺、觸覺、嗅覺、味覺等），以及他們所知道的事實進行陳述。但若是一個在其專精之領域或學科上符合一定資格之專家，則可以對其

所擁有專業知識之領域的範圍內，給予專家之意見。早期鑑識會計主要從事詐欺偵查與訴訟支援服務，近期擴展涵蓋舞弊風險管理，如擬定公司治理政策，發展詐欺防杜計畫，擬具公司犯罪處罰條款，或作為審計委員會之顧問等。（陳紫雲，民 95）。

（二）鑑識會計的工作流程

鑑識會計工作流程，劉麗真、王鈴（民 101）指出，其流程為構思證據→製作紀錄→蒐集證據→分析證據→報告及提出證據→確定證據。如圖 5。

1. 數位證據之蒐集：透過可靠的鑑識程序所蒐集之證據，獲得法院採納的機會很大。讓證據力最大化，包括：同時發生的事件、相關性及監管鍊（Chain of custody）。
2. 分析證據：分析證據的過程中，電子設備的處理應可能降低電腦記憶體靜止或損害的風險。如果有拆解設備的要求，必須採取適當措施，以確保該設備能夠返回到原有的功能，並可得到專家的幫助，解決內部文件標識符、用 Encase 軟體取得之影像。
3. 提供報告：鑑識審計結果應製作報告提供給客戶，報告內容應包括證據和結論的摘要，如果發現舞弊，應詳細揭露可能遭受損失的金額。如果沒有適當的控制，就可能產生舞弊。



圖 5 鑑識會計工作流程

資料來源：劉麗真（民 101），林宜隆、林榛麗（民 103）

五、數位證據鑑識標準作業程序

專業的鑑識人員，嚴謹的鑑識流程，以及專業的鑑識工具，能確保蒐集到的數位證據具有法律效力及避免同樣的證據產生不同的解讀。參考國外學者 Kuchta、Kruse & Heiser、Thomas Rude Eoghan Casey 及國內

學者林宜隆教授對於數位鑑識原則的觀點及看法，綜合專家學者對於數位鑑識程序的觀點，歸納出數位鑑識流程皆具有以下幾點：準備工作、收集、保存、分析、檢查、鑑定及報告呈現，如表 5。

表 5 鑑識作業程序比較分析表

學者	程序
Thomas Rude	1. 電腦鑑識準備工作 (Preparation) 2. 快照 (Snapshot) 3. 移轉 (Transport) 4. 實驗室鑑識準備工作 (Preparation) 5. 調查 (Examination)
Kruse & Heiser (美國學者)	1. 保存證據 2. 檢驗證據 3. 案件分析與陳述 4. 呈現結果
Kuchta (美國學者)	1. 準備工作 (Preparation) 2. 文件紀錄 (Documentation) 3. 收集 (Collection) 4. 鑑定 (Authentication) 5. 分析 (Analysis) 6. 保存 (Preservation) 7. 結果 (Production) 8. 報告 (Reporting)
Eoghan Casey (美國學者)	1. 準備與授權 2. 識別 3. 數位證據之保存、蒐集與記載 4. 過濾與數據簡化 5. 證據之分類、比對與個化 6. 證據恢復與犯罪現場重建 7. 報告結果

NIST SP 800- 101	1. 保存階段 (Preservation) 2. 萃取階段 (Acquisition) 3. 檢驗與分析 (Examination and Analysis) 4. 報告 (Reporting)
林宜隆 (國內學者) (2015)	1. 原理概念階段 (原則、法規、認知) 2. 準備階段 (權、安全政策、確定人事時地物、準備工具、專業人員訓練) 3. 操作階段 (蒐集、分析、鑑定) 4. 報告階段 (撰寫、呈現、驗證、法庭準備、建檔學習)

國內學者林宜隆教授提出數位證據鑑識標準作業程序 (Digital Evidence Forensic Standard Operation Procedure, DEFSOP) 結合國外學者的觀點與看法，故針對 DEFSOP 作探討。數位證據鑑識標準作業程序 (DEFSOP)，其程序包含原理概念、準備、操作及報告四階段，如圖 6。

(一) 原理概念階段：

1. 法規：數位證據的取得要遵循合法、真實的原則，當事人不得以非法侵入他人電腦資訊系統的方法獲取證據；證據取得的途徑必須以立法的形式規定取得數位證據的程序及許可權。
2. 原則 (IACC)：所謂的 IACC 原則是指必須保護
 - 完整性 (Integrity, I)：在不改變或破壞證物的情況下取得原始證物。
 - 正確性 (Accuracy, A)：證明所擷取的數位證據來自扣押的證物。
 - 一致性 (Consistency, C)：在不改變證物的情況下進行分析。
 - 符合性 (Compliance, C)：符合當地的法律規範。

(二) 準備階段：

主要工作是做一些鑑識前的準備

工作並蒐集相關資料，是為了操作階段各程序執行的預作準備，以下為其步驟：

1. 本階段的主要工作是做一些鑑識前的準備工作，並蒐集相關資料，蒐集犯罪對象基本資料：根據犯罪的類型，並利用已掌握的情況分析可能作案的人員，若案情需要也可訪談相關人員，並規劃鑑識執行的策略。
2. 決定搜索地點、對象與時間：根據犯罪的類型，並利用已掌握的情況分析可能作案人員，若案情需要也可訪談相關人員，另外再決定搜索地點、對象與時間，依據蒐集嫌犯資料後，決定搜索地點和時間。
3. 工具的準備：必需準備電腦軟硬體規格的參考手冊、犯罪工具程式的參考手冊及破解電腦。
4. 人員的專業性：對於一些鑑識工具的使用，鑑識人員必須具備專業性，也就是鑑識人員應該考取相關鑑識證照或認可，才不致於在鑑識過程中遺失寶貴的數位證據，甚至是破

壞掉數位證據。

5. 技術勤前教育：在每次出任務前，必須針對鑑識人員進行進一步的說明，說明搜索任務、項目，並檢查軟硬體及工具是否準備齊全，以避免一些意外狀況發生。

(三) 操作階段：

1. 蒐集程序：蒐集及備份數位證據，分為識別與記錄、保全與保存、收集與備份、搜索與扣押、打包與運送等五項工作。
2. 分析程序：搜尋及分析關鍵資料，在這個程序中可分為備份與紀錄、檢查與檢視、破解與搜尋、保管與分析四項。

3. 鑑定程序：擷取、比對及利用數位證據還原犯罪現場，在這個程序中將鑑定分為四個部分，分別為資料萃取、比對、個化、重建犯罪現場。

(四) 報告階段：

1. 撰寫、呈現及簡報：撰寫鑑識作業流程，註明使用工具及分類法，報告撰寫需詳實，簡報說明需用易讀圖呈現。
2. 驗證鑑識結果：證據檢驗及證據呈現需正確。
3. 法庭準備：出庭前人員及物證的準備。
4. 案件建檔及學習：案件資料庫建檔及案例教學教育。

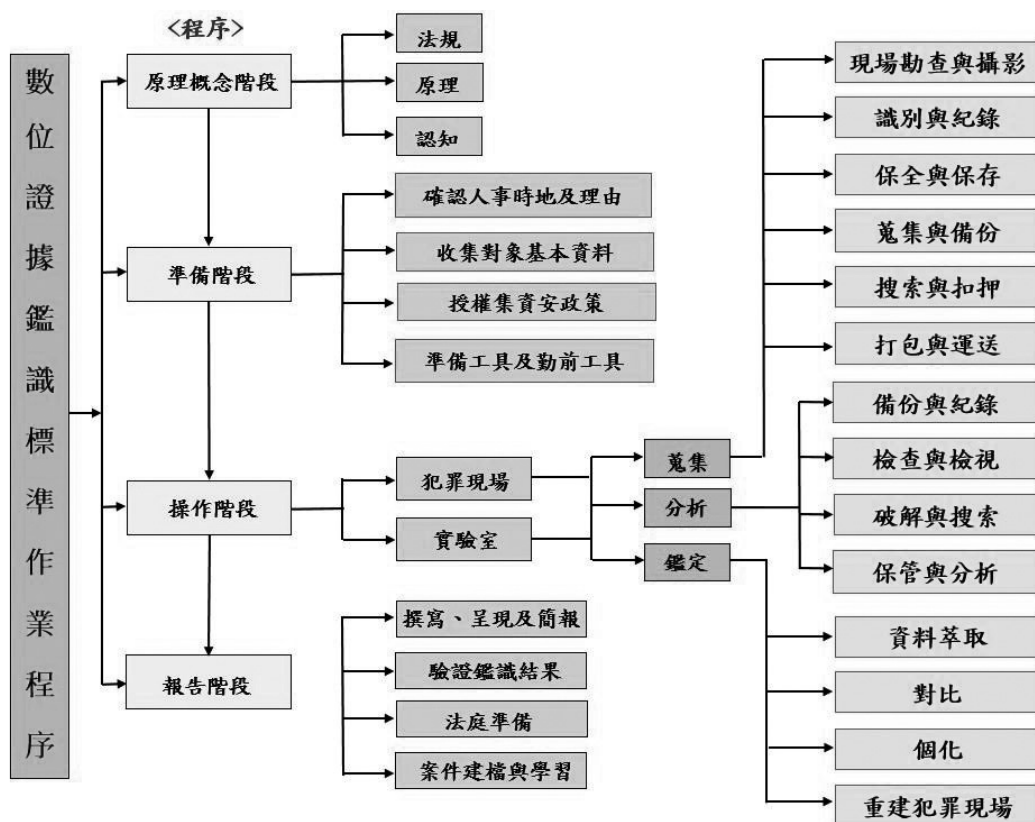


圖 6 數位證據鑑識標準作業程序

參、案例分析

一、整合民國 102 年～民國 107 年 6 月金管會銀行局重大裁罰案件

本次進行分析的個案來自民國 102 年 1 月至 107 年 6 月金管會銀行局所公布之重大裁罰案件，在公告資訊當中依案件性質可分為刑事案件、非重大裁罰及重大裁罰三種

不同之型態。根據近五年半的統計結果，在重大裁罰部分則有 110 件，裁罰對象除了付出數以百萬的罰鍰或者停止該項業務經營之代價外，所產生的營運缺失若未能獲得改善，更有可能增加未來經營風險。因此本文依案件內統計各年份的重大裁罰案件數，如圖 7。

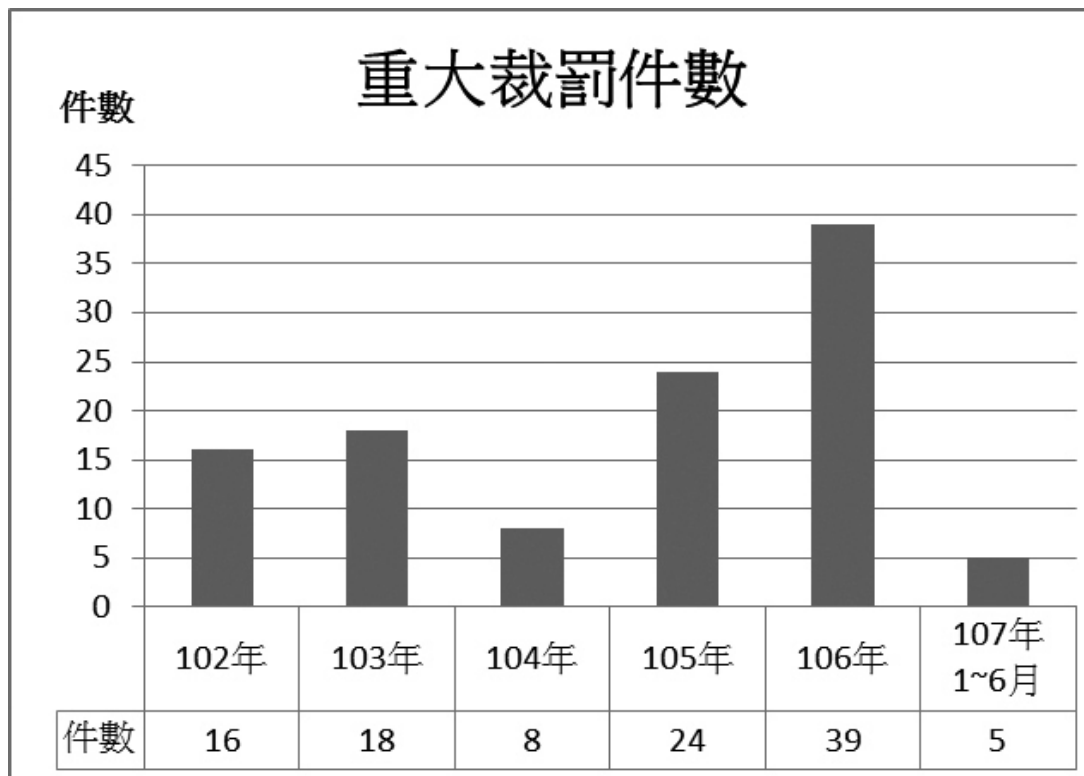


圖 7 重大裁罰件數統計

從圖 8、表 6 的內容中可看出，因為內部稽核的缺失（含內部稽核功能無法彰顯的情形）導致案件必然違反相關之法令規範，而遵循法令規範不但是業者基本的經營態度，也是內部控制制度規劃首要達成之目標，彙整 102 年～107 年 6 月裁罰金額少則

台灣工業銀行總裁罰金額 100 萬元，多則為中國信託金融控股股份有限公司（包含中國信託商業銀行）總裁罰金額 4200 萬元。由此可知，內部稽核無法有效監督運作業的項目，則所面臨的將是付出實質資產現金損失的代價。

圖 8 102 年~107 年 6 月裁罰金額統計

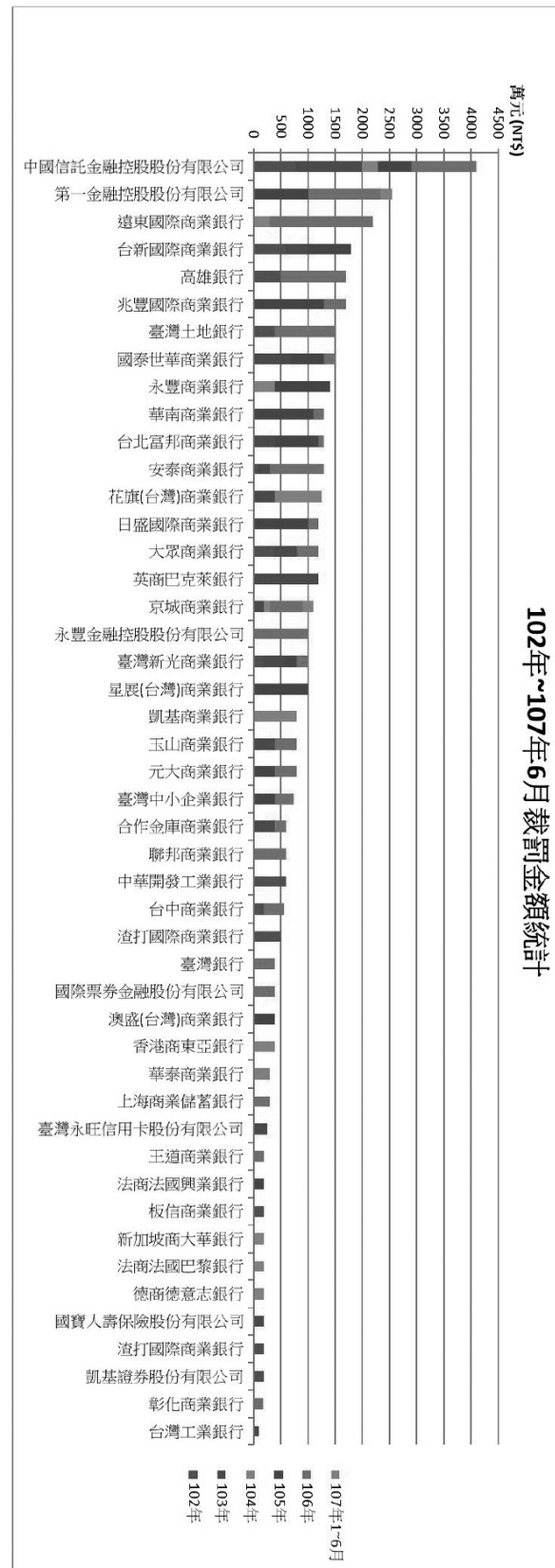


表 6 102 年~107 年 6 月裁罰金額統計

裁罰對象	102年	103年	104年	105年	106年	107年1~6月	Sub-total (萬元NT\$)	其他
中國信託金融控股股份有限公司	800	1200	300	600	1200		4100	
第一金融控股股份有限公司				1000	1340	200	2540	
遠東國際商業銀行			300		1900		2200	
台新國際商業銀行	600	400		800			1800	
高雄銀行	500				1200		1700	
兆豐國際商業銀行				1300	400		1700	
臺灣土地銀行	400				1100		1500	
國泰世華商業銀行		700		600	200		1500	
永豐商業銀行			400	1000			1400	
華南商業銀行				1100	200		1300	
台北富邦商業銀行		400		800	100		1300	105年解除職務
安泰商業銀行	100	200			1000		1300	
花旗(台灣)商業銀行		400				850	1250	
日盛國際商業銀行				1000	200		1200	106年停止職務
大眾商業銀行	400	400			400		1200	
英商巴克萊銀行		1200					1200	
京城商業銀行		200	100		600	200	1100	
永豐金融控股股份有限公司					1000		1000	
臺灣新光商業銀行	200	400		200	200		1000	106年停止職務
星展(台灣)商業銀行				1000			1000	
凱基商業銀行						800	800	105年暫停業務
玉山商業銀行		400			400		800	
元大商業銀行				400	400		800	
臺灣中小企業銀行				400	340		740	
合作金庫商業銀行		400			200		600	
聯邦商業銀行					600		600	105年暫停業務
中華開發工業銀行	600						600	
台中商業銀行	200				360		560	
渣打國際商業銀行	500						500	
臺灣銀行					400		400	
國際票券金融股份有限公司					400		400	
澳盛(台灣)商業銀行				400			400	
香港商東亞銀行			400				400	
華泰商業銀行						300	300	105年暫停業務
上海商業儲蓄銀行					300		300	
臺灣永旺信用卡股份有限公司		250					250	105年停止業務
王道商業銀行					200		200	
法商法國興業銀行				200			200	
板信商業銀行	200						200	
新加坡商大華銀行			200				200	
法商法國巴黎銀行			200				200	
德商德意志銀行			200				200	
國寶人壽保險股份有限公司		200					200	
渣打國際商業銀行	200						200	
凱基證券股份有限公司	200						200	
彰化商業銀行					180		180	
台灣工業銀行		100					100	

二、裁罰案件內部稽核缺失之分析結果

(一) 違反事實內容與營運作業項目之屬性分析

本節依據金融業營運作業項目分類案件違反事實內容的屬性，經初步分析案件違反事實內容與下列金融業營運作業項目有關：包括

投資準則、總務、資訊、人事管理、對外資訊揭露作業管理、金融檢查報告之管理、授信、新種金融商品及委外作業管理。彙整案件事實內容缺失的營運作業項目分類如表 7 所示。

表 7 案件事實內容缺失之營運作業項目分類彙整表

項次	違反事實內容之營運作業項目	小計
一	投資準則	6
二	客戶資料保密	8
三	利害關係人交易規範	4
四	股權管理	0
五	財務報表編製流程之管理	9
六	總務、資訊、人事管理	63
七	對外資訊揭露作業管理	9
八	金融檢查報告之管理	5
九	金融消費者保護之管理	19
十	重大偶發事件之處理機制	2
十一	防制洗錢及打擊資恐機制及相關法令之遵循管理	10
十二	其他業務之規範及作業程序	19

本由上表可知案件事實內容發生缺失最多的營運作業項目是在第六項「總務、資訊、人事管理」，共計有 63 件之多，其缺失內容主要係因為在資訊與人事管理的控制不周全，導致資訊未經合法授權而外洩，或

者是員工不當挪用資金、缺乏法令遵循的觀念以及盜用偽造客戶資訊進行違法行為。茲將各類型營運作業項目之統計比較圖繪製如下圖 9。

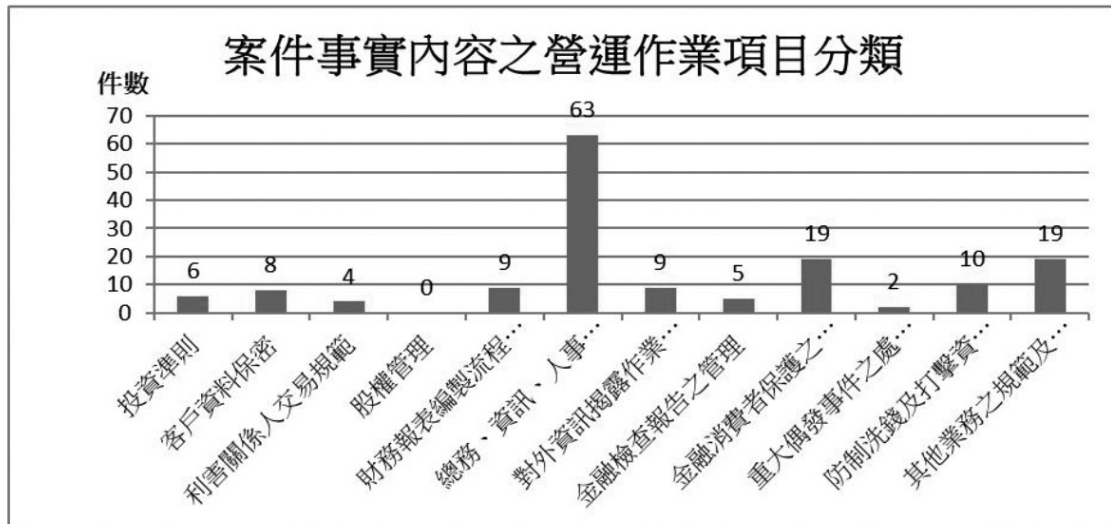


圖 9 案件營運作業項目缺失之統計圖

(二) 違反內部控制制度或未依規定執行相關內部控制制度
依據重大裁罰案件統計違反內部控制制度或未依規定執行相關內

部控制制度件數進行統計，如圖 10。未依規定執行相關內部控制制度逐年增加。

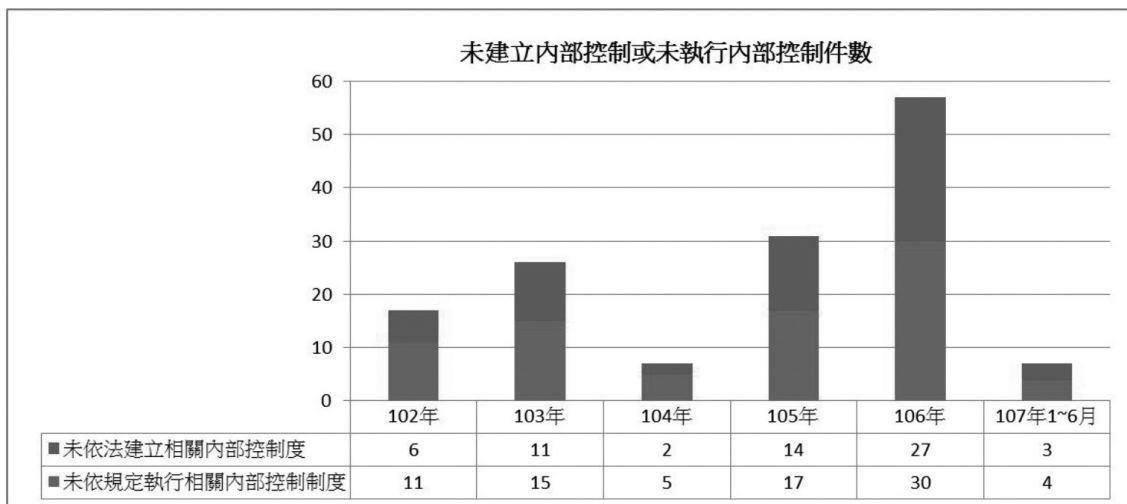


圖 10 違反內部控制制度或未執行內部控制之統計圖

(三) 內部稽核關鍵性查核項目
內部稽核人員是否能執行有效查核，有賴於是否採用適當查核程序與方法，查核內容必須能涵蓋

關鍵性查核項目，本文查核缺失擬定各營運作業項目的關鍵性查核項目，彙整如下表 8。

表 8 營運作業項目之關鍵性查核彙整表

項次	違反事實內容之營運作業項目	關鍵查核項目
一	投資準則	投資標的種類、核可與變動申報，投資金額上限
二	客戶資料保密	資料蒐集方式、資料儲存及保管方式、資料安全及保護方法、資料分類、利用範圍及項目、資料利用目的、資料揭露對象、客戶資料變更修改方式、選擇退出方式
三	利害關係人交易規範	定期更新關係人名單，特殊交易項目與金額之對象清查
四	股權管理	董事最低持股成數、股權異動申報、短線交易歸入權、避免內線交易及實施庫藏股期間股份賣出限制等事宜之規範與管理
五	財務報表編製流程之管理	會計科目之訂定是否符合相關法令規定、會計科目之分類是否適當、會計科目之增修是否經權責人員核准、會計事項是否取具合法憑證，無誤始進行過帳及結帳程序、是否採權責基礎入帳、財務報表內容是否依據一般公認會計原則編製、財務報表是否經權責人員簽核無誤、各項會計憑證、會計帳簿及財務報表是否依規定保存
六	總務、資訊、人事管理	資訊系統權限管理與權責區分、定期更換密碼及人員輪調、「金融機構安全維護管理辦法」建立管理機制、對ATM及網路連線之資安防護不足、汰換舊型機器、信用卡業務資訊系統暨資料處理委外及資訊設備採購作業、使用USB存取資料建立每日監視控管機制、重要資料保存程序
七	對外資訊揭露作業管理	制定對外資訊應揭露清單並定期依法令更新檢視
八	金融檢查報告之管理	依報告內容逐一檢視並取得佐證資料
九	金融消費者保護之管理	依不同金融商品之性質，設計消費者交易評估清單
十	重大偶發事件之處理機制	發生重大偶發事件通知治安或其他有關機關採取緊急補救措施
十一	防制洗錢及打擊資恐機制及相關法令之遵循管理	辨識、衡量、監控洗錢及資恐風險
十一	會計暨財務報表編製流程	覆核財務報表是否符合一般公認會計原則規範、財務報表附註揭露事項是否由專人負責收集及彙總相關資料
十二	其他業務之規範及作業程序	查核是否符合原則規範

(四) 數位證據鑑識標準作業程序設置建議

以圖9案件營運作業項目缺失之統的統計，最高是總務、資訊及人事管理的缺失，經關鍵查核項目建議多為資訊安全的管理缺失，故本文以此為例提出內部查核流程之設置建議。

以第一銀ATM盜領案為案例驗證，民國105年7月11日，國內金融史上首件ATM盜領案，第一銀行20家分行、51台ATM，7

月9日至11日，遭多名外籍人士盜領新臺幣83,277,600元，第一銀ATM盜領事件像是駭客直接從外部入侵造成的資安事件，發現其使用網路駭侵工具、吐鈔程式、滅證程式及連線中繼站IP等駭侵軌跡，提款機不正常吐鈔被國際犯罪組織盜領，但此事犯罪的發生，卻是因為其未能主動積極汰換舊型機器，而讓駭客有可趁之機。另外第一銀行無法在第一時間掌握損失的總金額，也顯

示出一銀在公司內部控制制度已出現漏洞。本案例運用林宜隆教

授提出的數位鑑識 (偵辦過程) 的方法分析，如圖 11。

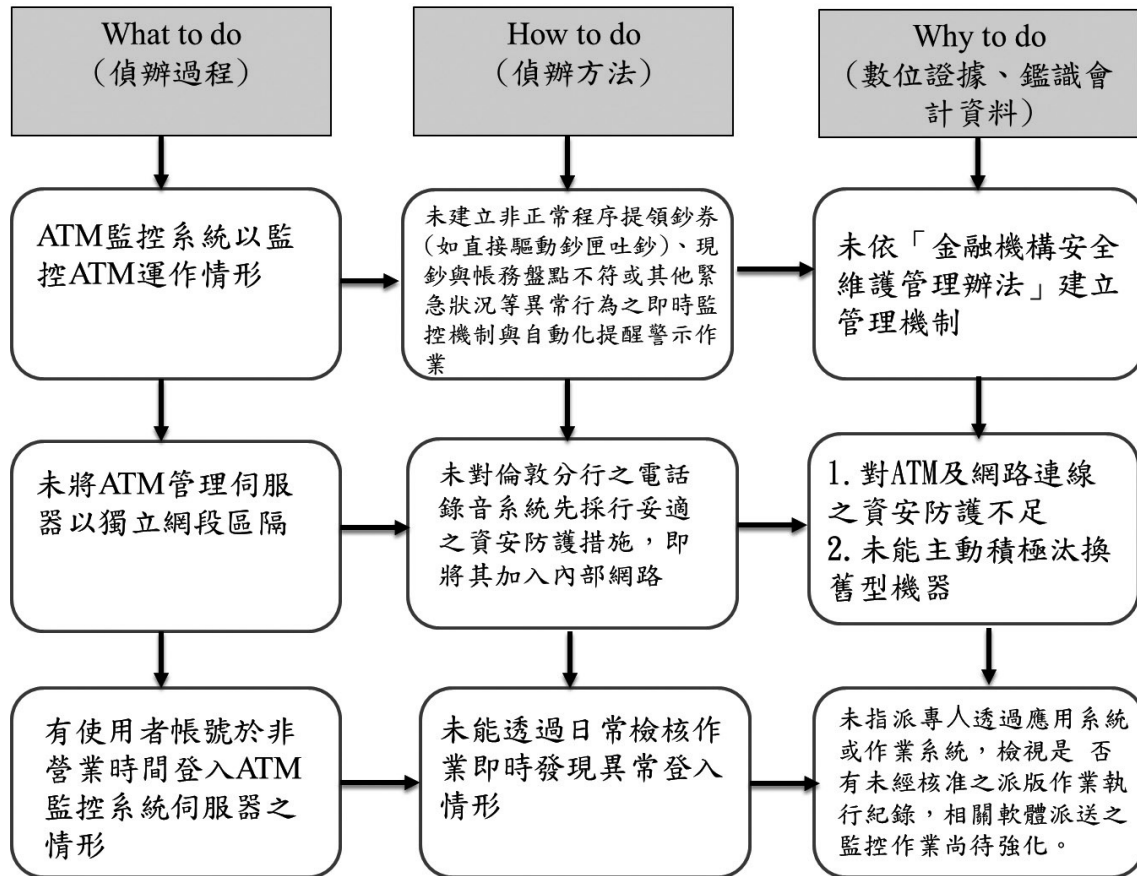


圖 11 數位鑑識 (偵辦過程) 的方法

由上圖 11 所示，鑑識過程運用了 What to do：發現了什麼線索，How to do：如何偵查，Why to do：由鑑識過程中經由分析得到的結果，幫助建立及確認查核方向和重點，並檢視工作流程的有效性。

由上述案中，分析其鑑識程序與所需規範暨相關知識如圖 12 所示，用以檢驗所建構之標準程序確實具有可行性。透過標準作業流程及規範、工具的標準化及認證。並就四大階段：原理概念階段、準備階段、操作

階段及報告階段，分別探討其重點工作、規範及流程，幫助稽核人員建立及確認查核方向和重點，並檢視工作流程的有效性。並配合主管機關銀行的三道防線。即事前預防 - 內部控制、事中應變 - 危機管理及事後處理 - 鑑識調查。讓內部稽核流程，從既有文件資料及假設，驗證過程中，尋找造成內部缺失之人、事、時、地、物，以釐清事實之原貌。

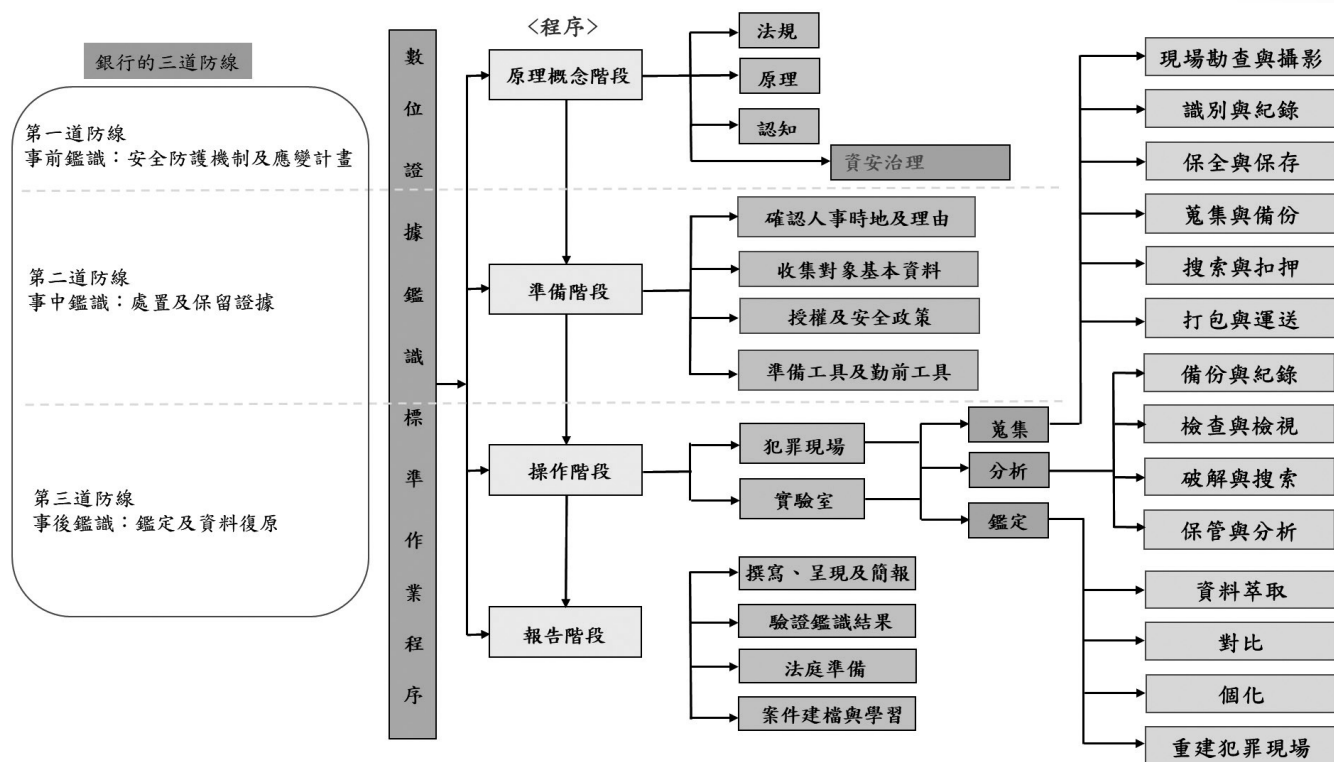


圖 12 數位證據鑑識標準作業程序設置建議

參考文獻

- 馬嘉應、蘇英婷，2007 年 4 月，企業舞弊的防制 (上)，會計研究月刊，第 257 期，第 43- 60 頁。
- 林宜隆，2009 年“網路犯罪：理論與實務”，中央警察大學出版社。
- 林宜隆、楊期荔，2011 年 1 月 1 日，鑑識會計簡介，電腦稽核期刊，第 23 期，頁 152- 153。
- 林宜隆，2012，建構數位證據鑑識標準作業程序 (DEFSOP) 與案例實證之研究電腦稽核，司法新聲，第 101 期。
- 林宜隆、林儂麗，2014，整合舞弊稽核與鑑識會計應用於政府會計之研究。
- 邱靜宜，林宜隆，2015 年 8 月 1 日，從金管會銀行局重大裁罰案件探討內部控制與內部稽核之缺失，電腦稽核，第 32 期。
- 林宜隆、潘彥臻，2016，從舞弊稽核與鑑識會計對兆豐銀行防制洗錢案之探討。
- 高照，認識舞弊三角加強內部監管，https://www.verity.com.hk/images/news/2015/bamboo_aug2015.pdf
- CNS 27014 中華民國國家標準 資訊技術 - 安全技術 - 資安治理
- 林宜隆，建構行動鑑識標準作業程序與整合國際鑑識標準，財團法人台灣網路資訊中心，2018 電子報 6 月份。

11. 林宜隆，電腦稽核、鑑識會計、數位鑑識與舞弊偵查及預防，中華民國電腦稽核協會二十周年專區。
12. 凱基銀交易員爆炒匯大虧 2.4 億開發金：虧損已帳列，<https://www.phew.tw/article/cont/phewpoint/current/topic/3766/201804243766>
13. 交易員炒匯大虧凱基銀被罰 800 萬 <http://www.chinatimes.com/newspapers/20180627000348-260205>
14. 裁罰案金管銀控字第 10701079801 號，https://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2&mcustomize=multimessages_view.jsp&dataserno=201806290001&aplistdn=ou=data,ou=penalty,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dttable=Penalty
15. 金融監督管理委員會主管法規共用系統，<https://law.fsc.gov.tw/law/index.aspx> 金融控股公司及銀行業內部控制及稽核制度實施辦法
16. 金融監督管理委員會，新版公司治理藍圖 (2018~2020)
17. 金融監督管理委員會，2013 年強化我國公司治理藍圖
18. 樊國楨、黃健誠，資安治理推動方案與落實電子化資安管理初探，Communications of the CCISA Vol. 15 No. 4 Oct. 2009
19. 孫強，資安治理，<http://202.99.120.116:82/gate/big5/publish.it168.com/2004/0617/20040617010101.shtml>，2004。
20. 黃明達、柯炫旭，政府機關資安治理之研究——以 x 政府機構為例，電腦稽核期刊第 22 期。
21. 林宜隆、楊慧茹，舞弊稽核與鑑識會計對內部控制缺失之探討 - 以凱基銀行外匯交易損失為例。電腦稽核期刊，第 39 期。
22. 林宜隆、楊慧茹，從金管會銀行局重大裁罰案件探討——內部控制與內部稽核之缺失。2017 Cyberspace 合研討會。中央研究院 資訊科技創新研究中心，台北市。
23. 林宜隆、楊慧茹，舞弊稽核與鑑識會計對內部控制缺失之探討 - 以凱基銀行外匯交易損失為例。TANET 2018 臺灣網際網路研討會，國立中央大學，桃園市。
24. 林宜隆、楊慧茹、李欣燕，從金管會銀行局重大裁罰案件探討銀行業內部控制缺失。2019 年第三十屆國際資訊管理學術研討會。輔仁大學。
25. 林宜隆，2015，雲端安全化及雲端鑑識化之新思維與新趨勢——雲端安全化，更要雲端鑑識化，台網中心電子報。
26. 高照，認識舞弊三角加強內部監管，https://www.verity.com.hk/images/news/2015/bamboo_aug2015.pdf
27. 劉麗真 (民 101 年 10 月)，淺談公部門鑑識會計，內部稽核，第 80 期，頁 39-46。[28] 劉麗真、王鈴 (民 101 年 9 月 6 日)，2012 年國際內部稽核協會年會出國報告，頁 24-25 <https://www.coursehero.com/file/35433598/25%E5%BE%B7%E8%8F%B2%E6%B3%9Delphi-methoddoc/>
28. iThome，2016，『駭客入侵一銀 AMT 流程追追追』，7 月 25 日

29. 林宜隆、吳昆霖、施凱麟，2016/ 11/ 18，
應用犯罪偵查知識工程化於刑案偵查實
務之研究 - 以第一銀行 ATM 跨國盜領案
為例。2016 Cyberspace 聯合研討會，大
同大學，臺北。
30. 康維玲，2013，內部控制缺失、公司治
理與銀行經營績效關聯性之實證、公司
治理與銀行經營績效關聯性之實證研究
－以我國銀行為例，中國科技大學企業
管理研究所
31. Bowen, P. (2006) Information Security
Handbook: A Guide for Managers, NIST SP
800- 100, 2006- 10
32. Julia H Allen and Jody R Westby.
“Characteristics of Effective Security
Governance,” EDPACS, 2007.

Is BitCoin a reliable FinTech Tool?

TSE Woon Kwan Daniel

ZHOU Xinquan

CAI Xintong

LI Jingyi

SHANG Di

Abstract

The popularity of BitCoin has been reflected by its fluctuating exchange rate in the financial market. Because of its special useful characteristics, it has been adopted by growing amount of enterprises as one of the financial technology tools nowadays. On the contrary, some countries show strong skeptical attitude or even rejection towards it also because of its special characteristics which affect effective governance issues so much. In this paper, we first review the past literature for understanding the origin and nature of BitCoin and then perform detail analysis by dissection of its strengths and weaknesses. Finally, we come up with the security and auditing concerns.

Keywords : BitCoin, FinTech, Security, Auditing, Robustness, Flexibility, Auditability

I. Introduction

Financial Technology (FinTech) refers to an economic industry formed by a group of enterprises that use technology to make

the financial services industry more efficient. These FinTech companies are usually created with the goal of adapting and perfecting the large financial firms and systems that are not

technical enough to make products and services more efficiently and less costly. With the rapid booming of FinTech, Internet finance is changing into financial science and technology which reveals the new trend of the deeply integration between Internet and financial. It uses scientific and technological means to innovate financial industry and to improve the efficiency of financial services for reducing the cost of financial services through creative Internet solutions. This new mode of increasing customer experience will eventually bring a brand-new experience to investors. BitCoin is one of the key elements used in FinTech which successes critically rely on the sophistication of this fantastic element. However, the use of BitCoin has also introduced lots of application problems (<https://news.bitcoin.com/>). In this article, background of FinTech and BitCoin were investigated and then followed by the critical analysis of potential security and auditing problems brought by using BitCoin element.

II. Literature Review

The word “FinTech” literally means the combination of “finance” and “technology” which is similar to “marriage”. With the rapid development of Internet and information technology, FinTech has become very popular among experts, society and governments. Financial Stability Board (FSB) understands FinTech as financial innovation driven by technology (Wang et al., 2017) and it is one

of new business models, new technology applications, and new product services including both the front-end industry and back-end technology that has created great impact on financial market, financial institutions and financial services.

It has taken quite a long time for finance and technology to get ‘married’ though the public attention to FinTech increased rapidly since end of 2014. The FinTech entered into a new step gradually since the global financial crisis in 2008. Xie et al (2007) claimed that the evolution of FinTech pays more attention to the balance between potential benefits and potential risks, new challenges and opportunities in developing countries, particularly Asia.

Basically, the understanding of FinTech is divided into two types. One is that advances of science and technology, especially the improvement of information technology, have positive impact on financial structure. For instance, Mishkin (1999) believed that transaction cost and asymmetric information are fundamental driving force to drive the evolution of financial structure. The improvement of technology has greatly improved the information asymmetry that enables financial intermediaries to get more financing from less-informed investors to advance liquidity in financial markets. At the same time, advances of technology have dramatically reduced transaction costs which results to new financial services constantly emerging and expanding their market capacity.

With the BitCoin growing up around the world, the block-chain technology which is technical infrastructure of BitCoin is drawing public attention. The core advantage of block-chain is decentralization. That is to say, the block-chain technology could realize peer-to-peer transaction, coordination and cooperation basing on decentralized credit by applying encryption, timestamp, distributed consensus and economic incentive to provide solutions for centralized institution in which there are high costs, poor efficiency and unsafe data storage. In addition, the block-chain technology is considered as the fifth disruptive innovation in computing paradigm following mainframe, personal computers, internet, and social media. It is also the fourth milestone in the history of the evolution of human credit following blood relatives' credit, precious mental credit and central bank notes credit (Swan 2015).

The rapid development of block-chain arise extensive concern from government departments, financial institutions, technological enterprise and capital market. In 2016 January, the UK government released block-chain research report in order to actively improve the application of block-chain in financial and government affairs (Walport 2016). People's Bank of China held digital currency seminars to explore the feasibility of using block-chain technology to issue virtual currency in order to improve the efficiency, convenience in financial activities.

BitCoins are so far the most successful implementation of block-chain technology.

According to block-chain real-time monitoring website (Block-chain 2017), an average of 120,000 trades involving about \$ 75 million a day are written into the BitCoin block-chain and have generated more than 400,000 blocks. At present, the number of BitCoins mined is more than 15 million. Its total market capitalization is over \$ 5.9 billion ranking 144th in the world GDP during 2015 (Yuan & Wang 2016). In other words, decentralized BitCoin has relied on algorithmic credit to create a global economy comparable in volume to smaller European countries without the credit endorsement of the government and the central bank. It is estimated that by 2027, 10% of global GDP will be stored via block-chain technology.

III. Background of BitCoin

The BitCoin concept was first proposed by Nakamoto (2008) to design and release open source software based on Nakamoto's ideas with a point-to-point (P2P) network on it. The feature of P2P transmission indicates that it is a decentralized payment system. It is a digital currency generated by a distributed network system in P2P form which relies on distributed network nodes to participate in a consensus process known as Proof of Work (PoW) to complete the verification and record BitCoin transactions. The process of PoW is also called BitCoin mining and every node is called miner. Each node contributes its own computing resources to compete to

solve an adjusted mathematical problem. The miners who solve the mathematical problem successfully will get the accounting right of the block, and pack all BitCoin transactions for the current time period into a new chunk, chronologically linked to the BitCoin currency. At the same time, the BitCoin system will issue a certain amount of BitCoins to reward the miner and motivate other miners to continue contributing computing force. The circulation of BitCoin relies on cryptography to ensure security. The following figure shows the BitCoin ecosystem.

Compared with other currencies, BitCoin is not governed by a specific currency agency. It is generated through many different calculations which based on a particular mathematic algorithm. The BitCoin economy applies a distributed database of nodes in the whole P2P network platforms to make sure all transactions are recorded; it also uses cryptography to confirm the safety of all parts of currency circulation. Decentralization and algorithms themselves are able to ensure that currency is less likely to be manipulated by massively producing BitCoin. Designing with cryptography feature allows BitCoin will be just accessed or paid by the owner. This also promises the anonymity of ownership of currency and distribution transactions. The most significant difference between BitCoin and other currencies in our daily life is the number of scarcities: BitCoin has limited number of scarcities; BitCoin could be seen as the redeem money that can be changed into

most countries. Users are able to use BitCoin to buy some real-life items, like clothes, books and even outfit of online games. The monetary characteristics of BitCoin include decentralization, circulation around the world, exclusive ownership, low transaction cost, no hidden cost and multiple platform mining.

BitCoins are the result of the integration of cryptography with the current advances in Internet communication technology. It is a decentralized P2P digital currency, which is designed based on the encryption methods. As mentioned before, Internet and cryptography techniques are used to ensure the transfer speed and security of funds between the two parties without a third-party platform to grant credit. Transactions about BitCoin are not supervised by any government or institutions. It has the following security and auditing attributes:

3- 1. Security and anonymity

According to Nakamoto (2012), all of the financial transactions which can be achieved through the BitCoin network are all encrypted by public key. The system will produce two related private keys based on some mathematic ways. Then, encrypted private key cannot be used to decrypt the message. If user receives one of the private keys, another one could be passed publicly. When other people want to transport BitCoin to this account, he is required to input the public key. Then, public key will encrypt the payment activity; specified user is the only person who can decrypt the related private key transactions. Also, the payer must

admit this transaction by his own private key at the same time. For further improvement in terms of security, in every transaction, users should be allowed to create public addresses when it is essential.

3- 2. Decentralization

As a kind of digital currency, the build of BitCoin does not need any agencies or banks to deal with these transactions. Community of BitCoin could be treated as a bank; all of the users in this bank contribute their working efforts into this community. This feature makes it possible to finish centralized processing in the user's entire network the P2P technology. All of the exchange activities can be done through existing BitCoin procedure. According to Grinberg (2012), apart from that, decentralization system has another benefit, which is that hacker cannot get close to the real BitCoin platform effectively. The data related to BitCoin is dynamic and synchronized by the entire networking calculating ability. It is difficult to obtain the BitCoin data since excellent, beyond the whole network computing power is required. The possibility for individual or an organization to get the ability which exceeds the whole network is low.

However, cracking password by computer is not the only choice for hackers to steal the information. It is likely for them to steal user information in other ways, thus influencing the security of BitCoin. Generally, BitCoin system is safety, systems and software that can

integrate individuals into a stable community by P2P platforms. Furthermore, the design of the system makes it possible for new member who is willing to join the community freely, in other words, they will not be refused by anyone. Once people want to change the BitCoin system or community, the permission of most members is required, this ensures that a stable system of fair and democratic protection of the interests of users.

In larger virtual communities or software systems, virtual currency issuers rely on strong capital or goodwill to support the circulation of electronic money within a certain range. However, there is no guarantee of third-party credit in the circulation and distribution of BitCoin, and transaction security often depends on the credibility of both parties. In the event of any dishonesty on the part of the parties to the transaction, the legitimate rights and interests of the other party cannot be effectively maintained. Especially in cross-border transactions, because the transactions span across different jurisdictions, the two parties are far apart and trade in BitCoin without credit guarantee, the seller cannot guarantee that the buyer will be able to make the payment after the delivery, and the buyer will not be able to do so after the seller ensures the scheduled delivery. Such transactions, seemingly exempt from the middle of the bank exploit, but in essence a retrograde online payment mechanism. The behavior of both parties to the transaction is completely governed by credit. In the event of a dispute, the rights and interests

of both parties to the transaction are hard to be guaranteed.

IV. The strengths and weaknesses of the BitCoin

4- 1. Strengths

BitCoin helps the block-chain technology able to avoid nearly all the information security problems. Since the hash function is a one-way function, if the people who do not know the right information, then they will have no possibility to decrypt it. Take the Wanna-Cry as example again, why the attackers are willing to choose the BitCoins as the only currency they will receive? One of the most important reasons is the security and privacy. Since the BitCoin has been delivered to the attackers, there is no method that can trace the delivery trail if the receiver cannot provide the authentication; however, it is allowed in the BitCoin system. Therefore, it can be considered that the BitCoin is one of the safest way to do the transactions all over the world.

In the meantime, the use of digital signature and the timestamps provide the entity authentication that including the digital origin authentication and the freshness. These two cryptology can help people authenticate where exactly the BitCoin comes from and when exactly the BitCoin generated. These two characteristics help people perform the entity authentication, giving the confidence of the

whole transaction process.

In addition, the BitCoin transactions can happen at any time in any place. It will significantly reduce the transaction time in real situation. It is highly possible for one BitCoin transaction to be completed in only 10 minutes. The reason that the whole transaction time can be deducted is mainly because of the elimination of the traditional third agency between the seller and the buyer, such as the huge banks in between the transaction process. Furthermore, the transparency of the transactions record is open for all participants who are using BitCoins. All the payment records will be stored in the whole block-chain system, and everyone can check it if they want. Most importantly, the personal information of the seller and the buyer will not be included in the records, which means it is totally safe for the people who do not expect their private information leak out.

4- 2. Weaknesses

Every coin has two sides; the BitCoin is not an exception. Along with the people increasingly take part in this field, the negative side is starting to appear. At first, there is a limitation of the number of the BitCoin, which is at most 25 BitCoins will be mined per 10 minutes. Therefore, when the demand cannot be satisfied by the supply although the value of one BitCoin experienced dramatically rise in the past decade, the challenges of getting one BitCoin will be much difficult than before. The requirements of hardware are strict and the

entry barrier of this area is high as well which means the basic computer knowledge will be required.

Secondly, the governance of the BitCoin market is another problem which the government needs to take into account. Due to the coinage controlled by the “miners”, the government cannot manage the total number of the BitCoin. Similarly, the ability of implementing the corresponding policy will be lacked. At the same time, the BitCoin is not the legal tender in most of the countries, so it may impede its circulation when the transactions happen around the world. Furthermore, the hardware security must be considered as one of the most important issues for the users is the need to pay more attention. For instance, the data will be definitely lost if the hard disk is lost. Or even just forgetting password of your account, then your BitCoin will disappear. Besides, the exchange rate has a significant fluctuation after it was created, the real value of the BitCoin is hard to do the confirmation, the possibility of the miners or the consumer may experience a huge loss is high.

V. Potential Security and Auditing Problems of BitCoin

5- 1. Robustness

The BitCoin economy uses a distributed database of nodes across the P2P network to identify and document all transactions and

to use cryptography to ensure the security of all aspects of the currency flow. However, the robustness of the BitCoin is not that high. BitCoin and other attempts use block-chain and other technologies and conventions to ensure the scarcity of currency, thus challenging the current financial system of bankruptcy. However, the price of BitCoin has been highly volatile. According to statistics, its volatility is more than seven times that of gold, more than eight times the stock market index such as the S & P 500 index. Such volatility poses a greater risk that it will not be able to serve as a means of value storage nor as a unit of account for general merchandise. Moreover, the agreement that the total number is permanently limited to 21 million and decentralized also limits the BitCoin's management functions in the socio-economic implementation.

According to Grinberg (2012), BitCoin transactions rely on encryption and block-chain technology. However, the current BitCoin system does not yet guarantee the security of individual who owns BitCoin in its own storage and exchange of national credit money. The choice of wallet and trading platform is like the choice of banknotes for all commercial banks and clearing center. BitCoin was stolen for the most part, with Mt.Gox, the world's largest BitCoin exchange operator, bankrupt in February 2014. At that time, 850, 000 BitCoins in the trading platforms were stolen by hackers, with an estimated loss of about 467 million U.S. dollars. In August 2016, Bitfinex, the Hong Kong-based digital currency exchange,

stole 119,756 BitCoins at a total value of about 75 million U.S. dollars. As a result, the BitCoin prices fell about 25%. Therefore, the robustness of the BitCoin is not that stable for any investments, sometimes the fluctuation even much bigger than purchasing a stock.

The processing of BitCoin is complicated. In order to ensure that there is no double payment, the BitCoin needs to be as follows:

- (1) All transactions open to the public
- (2) Need to have a time stamp, all transactions are in order
- (3) The need for additional resources to confirm the transaction

History of the whole network open, then each account there are how many BitCoin, not by a data to represent, but based on historical transactions derived. The history of the transaction chain is recognized through the entire network, in order to ensure that not be faked. All transactions, according to the order, to be timestamped, the previous transaction is successful, the entire transaction chain is recognized, the next transaction is based on the last transaction to generate, the entire transaction is a transaction chain, In order to ensure that not be double pay.

The confirmation of the transaction needs some powerful resources to support it. This introduces a work load proof that more than 50% of the whole network can prove the validity of a transaction. If someone wants to tamper with a previously completed transaction, it becomes difficult. So from the transaction point of view, the entire system is

very stable.

But on the other hand, the product is very unstable for BitCoin. Price rose rapidly. As a commodity, BitCoin has fluctuated in price in just a few years. From the beginning of 2009 to the beginning of 2010, BitCoin was of no value. In the first half of 2010, when BitCoin began trading in the first half of 2010, the value of 1 BitCoin was less than 14 cents. In the summer of 2010 BitCoin transactions started to enter the golden age. Due to the disparity between supply and demand, the online transaction value Start to rise. By early November, BitCoin rose to 36 cents after a long silence at 29 cents. The exchange rate with the U.S. dollar reached a 1: 1 exchange rate in February 2011, stabilizing at 87 cents and rising to over 1.06 U.S. dollars. In the spring of 2012, BitCoin reported "big bang" growth after Forbes covered "cryptocurrency." From early April to late May, it rose from 86 cents to 8.89 U.S. dollars. Then, on June 1, it went 3 times in a week to reach 1 dollar for 27 dollars. On April 10, 2013, BitCoin touched \$ 266 all the way, dropping to \$ 50 in just a few days and quickly returned to around \$ 140. This shows that the range of price changes of BitCoin is very large, which is a huge challenge to its robustness.

It has been controversial since BitCoin came out in 2009. Every coin has two sides. There is no doubt that the advent of BitCoin is disruptive but some problems about robustness of BitCoin are brought up. The following analysis about BitCoin robustness is divided

into two parts: market value and risk of technology.

The value of BitCoin depends on how many people, how many goods and services are willing to accept BitCoin payments. If the number of people who receive BitCoin increases, BitCoin will have a huge appreciation of space. In the real world, the exchange rate between BitCoin and the U.S. dollar is very volatile. This virtual currency has added 5000 times within three years. In 2013, one BitCoin was worth more than 260 U.S. dollars, and plummeted to 130 U.S. dollars. However, the value of one BitCoin has reached up to 11, 134 U.S. dollars (2017/12). There are only a few hundred million people who own BitCoin at present, which has great room for growth compared with the billions of Internet users, which is also the reason that most current BitCoin holders are very confident. The hitting turbulence of BitCoin value brings the related risks to BitCoin holders.

When BitCoin is described as a decentralized system, one of the key assumptions is: No single individual or organization can control most of the computing power of BitCoin. If any individual or organization has 51% of the BitCoin network's computing power, it can actually control the whole BitCoin network. Ignoring the blocks created by the other 49% nodes, the amount of CPU required to control 51% of the BitCoin network would be an astronomical number. It seems that BitCoins that are stored solely on

source code may not be retrieved once they have been stolen. In principle, BitCoin trading system is any site that can participate; the security of its transactions entirely depends on the site's self-regulation and the ability to deal with hacking. BitCoins have high anonymity, which makes it hard to trace once the stolen issue has occurred. All the losses can only be borne by the victims themselves, so they are much concerned by hackers. There are some technical issues that BitCoin systems have to overcome. As more and more people enter, the amount of data flowing between users will also increase which will reduce the overall system speed. Although this problem can be solved by posting patches, patches are hard to come by. The rapid increase in the use of BitCoin will endanger its own development.

5- 2. Flexibility

Certainly, the BitCoin has the flexibility when people begin to use it. Because anyone can do the BitCoin transactions at anywhere in any time, this advantage of the BitCoin is obvious. BitCoin is more flexible than traditional currency. BitCoin is a new payment method designed to give customers more flexibility. BitCoin payments can be easily made anywhere in the world and the payment processing costs are reduced. BitCoin is a kind of electronic money which is based on the background of big data, cloud computing and artificial intelligence. With the development of these technologies, the financial field is more dependent on the Internet. With the gradual

development of BitCoin, big companies are starting to accept BitCoin for their products, so their agility is beyond doubt. BitCoin can be used to do many interesting things and the number of retailers receiving the currency is also growing, especially in countries where digital currency is backed by regulators. However, it should be pointed out that the mainstream use of BitCoin as currency is still a distant dream. We can only hope that with BitCoin, the world's first digital currency rises in value, consumers and businesses will be more interested in it.

5- 3. Auditability

The auditability can be divided into two parts, which are the internal audits and the external audits. Ordinary online transactions, the authority of the center to determine the effectiveness of the transaction, for example, the bank's online banking, and banks act as the role of the bank to prove the validity of a transaction. Then, a bit like the election, voting by everyone, the most votes in the transaction, will be recognized as a legitimate transaction. Without an authority center, it seems that there is a lack of credit. However, the transactions resulting from voting are the most trustworthy. Thus BitCoin is also known by "democratic currency." In BitCoin's algorithm, voting is not a one person vote but a CPU one vote. So, if a person wants to control BitCoin, the TA must have enough CPU, then the bigger the BitCoin, the harder it will be to control. Like a person who can easily control hundreds or thousands

of votes, and the larger the size of the vote, the harder it will be to control.

In addition, when doing this type of voting, assuming that the workload is small, and then the confirmation that the transaction requires only a small amount of computing power can be completed which leads to the forgery of such transactions and is also very simple, so BitCoin is introduced PoW mechanism. In this mechanism, to prove a transaction, it takes a certain amount of computing power and time. Once the operation is successful, a transaction is determined. In turn, the average client, as long as a very simple operation, you can know this transaction is real or fake. This kind of mechanism is just like in real life, the government spends a lot of manpower on banknotes to carry out anti-counterfeiting treatment and the ordinary people only need to make simple identification of banknotes, they can identify genuine and fake.

In BitCoin, this algorithm of workload proof mechanism is called hash cash. In fact, this algorithm has long existed. Its principle is to find a random number in the transaction data block which contains a number of 0, the computer can only be an exhaustive approach to find this random number. If we ask for a random number, as the number of 0s increases, the computational workload increases exponentially. Once we find this random number, we determine a data block. The data block cannot be changed unless a certain amount of workload is calculated. Because of

this hashing algorithm, which is an exhaustive method, if the honesty node on the network exceeds 50%, basically the forger wants to fake a transaction and it will have a very low chance of success but there is still a chance!

In this case, BitCoin introduces another mechanism called the transaction chain. All the transactions are time-stamped and linked together in a chain. Like a rope above the rope hit a lot of knots, each knot represents a transaction and each knot in time is a sequence. The longest chain is recognized as a real transaction. A counterfeiter with a computing power of less than 50% wants to fake a transaction, and then has a certain probability. If he wants to fake two transactions and is faster than an honest one who is more computationally efficient, the probability is lower. Over time, the odds of success have dropped exponentially.

BitCoins also introduce a reward mechanism, when honesty nodes calculate a data block; it can get a certain amount of BitCoin rewards, BitCoin rewards honest mining more often than forged transactions. Because of these coping strategies, BitCoin transactions are a form of transaction that is open, transparent, unchangeable and vulnerable. So BitCoin is a very auditable currency.

BitCoin is designed to bypass any existing or institutional regulation. This is a serious discrepancy with the regulatory needs of the legal tender. Due to the lack of regulatory mechanisms, no institutions or organizations

make credit endorsements for BitCoin which is prone to frequent violent currency fluctuations, and use BitCoin to breach tax evasion, extortion money laundering and other crimes. Moreover, the increasing popularity of BitCoin continuously erodes the monetary sovereignty of all countries and even invalidates macroeconomic regulation and control policies carried out by currency issuance and circulation (BitCoin Strategy 2018). Because of this, most countries are cautious about the flow of BitCoin in their countries. They accept BitCoin at the same time proposed to strengthen the regulation of BitCoin. Criminals exploit the identity information disclosure of users in the BitCoin system to launch extortion and other attacks. They do not need to uniquely identify the owner of the BitCoin account, and only reduce the target attack object to a certain extent. In contrast, for government regulatory or judicial investigations, you need to uniquely identify the owner of an account and be able to associate all other accounts of the user.

VI. Conclusion

In 2016, the Internet finance industry, essentially the use of BitCoin, has become legal and standard and the government's regulatory policies on the financial technology industry became more and more stringent. While regulators are likely not to regulate Internet finance and financial technology separately, most financial technology companies also conduct their financial business through

Internet channels. But those who engage in legal franchise business, even if there is no entry requirement, also need to accept self-discipline management and record with national industry self-discipline organization.

In terms of scope, financial technology contains the concept of Internet finance but its essence is finance and the core of finance is wind control. Based on the data, using the innovative technology to reduce the cost of financial enterprises and extract the useful information from the data to assess the credit, avoiding fraud and credit risk is the two most highly appreciated practical imaginations in the financial technology at present. Although this kind of imagination has been realized by many companies, how to share and integrate multi-party data within the industry is also a challenge.

In this article, efforts have been spent to analyze the potential problems of BitCoin and got the findings of potential threats in terms of robustness, flexibility and auditability. In such, use of BitCoin can bring so many benefits to the financial market but it has to be closely monitored especially in governance issue because of the possible black market dealings inside. In other words, the government should not ban the use of it but it has to be carefully implemented and monitored once it will be used in more mission critical applications.

References

- 1.BitCoin Strategy , 2018, Behind Bitcoin: Who owns the Bitcoin Project?, bitcoin.strategy.io.
- 2.Block-chain Monitoring Website Available at < <https://www.block-chain.com/>> 2017. 12
- 3.Grinberg , 2012, Bitcoin: An Innovative Alternative Digital Currency, Hastings Science & Technology L.J.
- 4.Mishkin , 1999, Global Financial Instability: Framework, Events, Issues, Journal of Economic Perspectives Vol. 13, No. 4, Fall 1999 (pp. 3- 20).
- 5.Nakatomo , 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/en/bitcoin-paper>.
- 6.Swan, M. , 2015, Block-chain: Blueprint for a new economy. O'Reilly Media, Inc.
- 7.Walport, M. , 2016, Distributed Ledger Technology: Beyond Block-chain. UK Government Office for Science (p. 19). Tech. Rep.
- 8.Wang Guangyu, He Junni , 2017, The Responsibility and Future of Financial Technology, Journal of Southern Finance.
- 9.Xie Hui, Wang Jian , 2016, Study on Block Chain Technology and Its Application, Netinfo Security 9, pp 192- 195.
- 10.Yuan Yung 袁 勇 , Wang Fei Yiu 王 飞跃 , 2016, 区块链技术发展现状与展望 . 自动化学报 , 42(4), 481- 494.

中華民國電腦稽核協會

中華民國電腦稽核協會（CAA）自民國 83 年成立，舉辦過無數次有關資訊安全管理與電腦稽核等相關學術研討與實務運用之座談會，並舉辦各項資訊安全與電腦稽核講習課程，提供會員與外界人士一個提升專業知識及能力與分享經驗的場所。民國 85 年 ISACA TAIWAN CHAPTER 成立，為全球第 142 個支會，成為引領台灣與世界電腦稽核之先河，長期推廣國際電腦稽核師證照 (CISA)、國際資訊安全經理人證照 (CISM)、國際企業資訊治理師 (CGEIT)、國際資訊風險控制師認證 (CRISC)。民國 90 年與 BSI 開始合辦主導稽核員訓練及建置實務…等課程，例：資訊安全管理系統主導稽核員證照 (BS 7799/ISO 27001 Lead Auditor)、IT 服務管理系統主導稽核員證照 (ISO 20000 Lead Auditor)、營運持續管理系統主導稽核員證照 (ISO 22301 Lead Auditor)…等，並配合政府各階段 ISMS 的推動計畫，承辦國家資通安全標準的翻譯專案，且已成為證券期貨局、銀行局銀行業、銀行局票券商、投信投顧公會及保險局認可之內部稽核人員專業訓練機構暨公務人員終身學習訓練機構。

協會簡介

願 景

願景：持續為資訊科技治理與電腦稽核之先導機構。

宗 旨

- 一、推動電腦稽核及系統控制安全之學術研究發展。
- 二、協助制訂電腦稽核、控制、安全之標準。
- 三、協助企業強化電腦系統之控制與電腦稽核功能。
- 四、與國際電腦稽核相關組織作資訊及技術之交流。
- 五、協助保護個人資料等事項。

任 務

- 一、舉辦有關電腦稽核、控制、安全之研討會、講習會。
- 二、舉辦企業及機關團體之教育講習，以推廣有關電腦稽核控制，安全之實施。
- 三、出版電腦稽核、控制、安全之刊物及著譯叢書。
- 四、聯繫企業、學術界及政府機構，以促進電腦稽核理論與實務之交流。
- 五、接受企業、政府機構委託協助建立電腦稽核功能與電腦安全及控制制度或辦理電腦稽核之研究。
- 六、舉辦對電腦稽核有貢獻之表揚事項。
- 七、接受政府相關機關之委託舉辦電腦稽核人員資格檢定。
- 八、聯繫國際電腦稽核組織、進行合作。
- 九、辦理其他為達成本會宗旨之必要事項。

沿革

- 1994 年 7 月 14 日正式創立，由朱寶奎擔任第一屆理事長。秘書長由林秀玉會計師擔任。
- 1996 年 7 月由朱寶奎續任第二屆理事長。秘書長由林秀玉續任。
- 1998 年 7 月由魏忠華接任第三屆理事長。秘書長由陳瑞祥擔任。
- 2000 年 8 月由魏忠華續任第四屆理事長。秘書長由黃淙澤擔任。
- 2002 年 9 月由蔡峰霖接任第五屆理事長。秘書長由莊盛祺擔任。
- 2004 年 9 月由吳琮璠接任第六屆理事長。秘書長由吳素環擔任。
- 2006 年 9 月由吳琮璠續任第七屆理事長。秘書長由許林舜擔任。
- 2008 年 9 月由黃明達接任第八屆理事長。副理事長由林宜隆擔任。秘書長由徐敏玲擔任。
- 2010 年 8 月由黃明達續任第九屆理事長。副理事長由林宜隆續任並暫代秘書長。
- 2012 年 8 月由林宜隆接任第十屆理事長。副理事長由楊期荔擔任。秘書長由黃淙澤擔任。
- 2014 年 8 月由林宜隆續任第十一屆理事長。副理事長由楊期荔續任。秘書長由黃淙澤續任。
- 2016 年 8 月由張紹斌接任第十二屆理事長。副理事長由蘇庭興擔任。秘書長由黃淙澤續任。
- 2018 年 9 月由張紹斌接任第十三屆理事長。副理事長由蒲樹盛擔任。秘書長由黃淙澤續任。

會員權益

- 一、可免費參加本協會定期舉辦之例會活動(含台北、新竹、南區)，並獲得 CISA、CISM、CRISC 及 CGEIT 持續進修(CPE)學分。
- 二、參加 CISA、CISM 國際證照考試複習課程及本協會舉辦之課程可享有會員折扣價。
- 三、會員得以優惠價格購買協會出版品。
- 四、可免費獲得協會出版之《電腦稽核期刊》(一年兩期)。
- 五、透過電子郵件方式，可取得電腦稽核相關領域之最新訊息。
- 六、輔導會員取得國際電腦稽核師(CISA)、國際資訊安全經理人(CISM)、國際資訊風險控制師認證(CRISC)及國際企業資訊治理師(CG EIT)證照並提供會員專業認證管道。
- 七、參加協會各種活動、擔任協會委員會委員及出席會員大會等，並享有發言權、表決權、選舉權、被選舉權；團體會員得由五位代表人出席本協會會議並行使權利義務。
- 八、可進入協會會員專屬網站瀏覽各期刊物及下載各類電子文檔，如歷年期刊文章、ISACA 摘譯期刊、例會講義、職業道德規範、及提供各項查核指引等資料。

會員義務

- 本協會會員有繳納會費及遵守本會章程與決議事項之義務。

2019 下半年度教育訓練課程列表


電腦稽核協會為證期局公發公司、銀行局金控公司及銀行業、信用卡業務機構、電子支付機構、保險局保險業、保險代理人/經紀人公司、投信投顧公會認可之內稽人員訓練機構及董監進修課程辦理機構及公務人員終身學習訓練機構

課程類別	課程主題	時數	預定開課時間	課程費用
ISACA 國際證照系列	CISA 國際電腦稽核師認證研習班_平日班	30	9/11-12、18-20	NT\$ 30,000
	CISM 國際資訊安全經理人認證研習班_假日班	18	9/7、21、28	NT\$ 18,000
	CISM 國際資訊安全經理人認證研習班_假日班 (與金融研訓院合辦，上課地點：研訓院)	18	10/19、26、11/2	NT\$ 18,000
ISO 系列	ISO 27001:2013 資訊安全管理系統 CQI & IRCA 主導稽核員訓練課程	40	11/11-15、12/9-13 假日班：10/17-19, 25-26	NT\$ 53,000
	ISO 27001:2013 資訊安全管理系統 建置實務課程	24	10/16-18	NT\$ 36,000
	ISO 22301:2012 營運持續管理系統 CQI & IRCA 主導稽核員訓練課程	40	11/11-15	NT\$ 55,000
	ISO 22301:2012 營運持續管理系統 基礎課程	16	12/2-3	NT\$ 21,000
	ISO 20000-1:2018 IT 服務管理系統 CQI & IRCA 主導稽核員訓練課程	40	12/23-27 高雄班：12/23-27	NT\$ 55,000
	ISO 20000-1:2018 IT 服務管理系統 CQI & IRCA 主導稽核員訓練轉版課程	16	11/25-26	NT\$ 22,000
	ISO 20000-1:2018 IT 服務管理系統 建置實務課程	24	12/2-4	NT\$ 35,000
	ISO 29100:2011(CNS 29100)隱私框架 主導稽核員訓練課程	36	11/4-8	NT\$ 55,000
	ISO 29100:2011(CNS 29100)隱私框架 國際標準基礎課程	8	10/21	NT\$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準建置課程	16	10/7-8、12/16-17	NT\$ 15,000
內稽系列	運用 80/20 法則有效進行稽核工作(新竹班)	6	10/5	NT\$ 3,300
	內部稽核有效應用財務報表實務班(初任課程)★	6	10/21	NT\$ 3,300
	☐實作持續性稽核平台—以 ACL 與 Excel 為例	6	10/28	NT\$ 3,300
	內部稽核實作基礎班(初任課程)	12	11/11-12	NT\$ 6,600
	☐應用簡報視覺化技巧呈現經營管理與稽核報告	7	11/25	NT\$ 3,850
	☐電腦查核加班費特休假與輪排班_新法規一例一休試算範本	7	11/26	NT\$ 3,850
	內控 2.0：統計預測、數據分析、資訊安全與舞弊偵防★	6	12/20	NT\$ 3,300
IT Audit 與資訊治理系列	☐從 Big Data 偵測資料以預警防弊與興利_資料處理初級課程	15	9/24-25	NT\$ 7,500
	☐從 Big Data 偵測資料以預警防弊與興利_樞紐分析進階課程	15	10/15-16	NT\$ 7,500
	☐從 Big Data 偵測資料以預警防弊與興利_查核六大循環作業	15	10/23-24、12/18-19	NT\$ 7,500
	☐從 Big Data 偵測資料以預警防弊與興利_企業銷售查核作業	15	11/28-29	NT\$ 7,500

課程類別	課程主題	時數	預定開課時間	課程費用
IT Audit 與資訊治 理系列	☐從 Big Data 偵測資料以預警防弊與興利_圖表製作進階課程(初任課程)	15	12/26-27	NT\$ 7,500
	☐從 Big Data 關聯式資料查核 Power BI_透視視覺化圖表分析	7	9/17	NT\$ 3,850
	☐從 Big Data 偵測資料以預警防弊與興利_資料處理基礎課程(初任課程)	7	10/22、12/23	NT\$ 3,850
	☐從 Big Data 偵測資料以預警防弊與興利_樞紐分析基礎課程(初任課程)	7	10/29	NT\$ 3,850
	☐提升電腦專業查核_匯總 Excel 屏東不用函數避免當機	7	11/21	NT\$ 3,850
	新時代稽核變革及實務案例分享★	6	9/23	NT\$ 3,300
	以數據分析解析營運流程與財務舞弊偵測★	6	10/3	NT\$ 3,300
	談資安事件應變機制及稽核重點★	6	10/4	NT\$ 3,300
	數位時代電腦稽核實務研習(初任課程)★	6	10/7	NT\$ 3,300
	作業系統與通信傳輸查核★	6	10/8	NT\$ 3,300
	ERP 系統控管與查核實務★	6	10/9	NT\$ 3,300
	☐稽核分析在金融業以風險為導向內部稽核個案演練(Arbutus 上機操作)	6	10/18	NT\$ 3,300
	資訊時代稽核專業職能與倫理規範★	6	11/4	NT\$ 3,300
	網站安全與稽核簡介(I)★	6	11/6	NT\$ 3,300
	資訊部門稽核與資訊系統控制查核★	6	11/7	NT\$ 3,300
	網路與系統安全實務查核★	6	11/8	NT\$ 3,300
	有效成本管控設計與分析★	6	11/15	NT\$ 3,300
	鼎新 Workflow ERP 系統控管與查核實務	6	11/27	NT\$ 3,300
	金融 3.0 的創新應用與風險管理★	6	12/4	NT\$ 3,300
	網站安全與稽核簡介(II)★	6	12/6	NT\$ 3,300
舞弊稽核 與數位鑑 識系列	舞弊查核資料分析實務	6	9/16	NT\$ 3,300
	資安持續稽核與監控：組態安全管理之應用★	6	9/26	NT\$ 3,300
	資安事件與資料外洩調查實務分享★	6	9/27	NT\$ 3,300
	應用鑑識資料分析(FDA)技術查核財務舞弊★	6	11/1	NT\$ 3,300
	內部稽核舞弊偵查應用技巧實作班(初任課程)★	6	11/18	NT\$ 3,300
	全面舞弊風險管理－從預防、偵測、調查到危機處理★	6	11/19	NT\$ 3,300
	NEW!數位鑑識技術基礎與實務	6	11/22	NT\$ 3,300
	數位證據與實例分享★	6	12/11	NT\$ 3,300
	結合系統資料與網路資源透析潛在舞弊事件	6	12/16	NT\$ 3,300
個資外洩 與保護系 列	資料庫稽核與個資保護★	6	10/17	NT\$ 3,300
	個人資料保護稽核★	6	12/13	NT\$ 3,300
數位金融 與電子支 付系列	以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循★	8	12/13	NT\$ 8,000

※ 本會保有課程安排及師資調整異動之權利，實際課程請依本會網站公告為準。

※ 本會會員課程費用另有優惠。

※ 「」為上機操作課程，學員需自備有 USB 孔的筆電。

※ 「★」為上市上櫃公司董事、監察人進修課程。

※ 可申報進修時數：實際可申報時數請依本會網站公告為準。

- | | |
|--------------------------------|-------------------------------------|
| ■ 證期局公開發行公司內部稽核人員訓練時數 | ■ 保險局保險業內部稽核人員在職訓練時數 |
| ■ 證券期貨局內部稽核人員初任職前訓練時數 | ■ 保險局保險代理人及保險經紀人內部稽核人員在職訓練時數(今年無申報) |
| ■ 證券期貨局內部稽核人員在職或替代訓練時數 | ■ 投信投顧公會內部稽核人員訓練時數 |
| ■ 銀行局金融控股公司及銀行業內部控制及稽核人員在職訓練時數 | ■ 公務人員終身學習時數(限 ISACA 證照及 ISO 課程) |
| ■ 銀行局信用卡業務內部稽核人員在職訓練時數 | ■ CISA、CISM、CGEIT、CRISC、CIA 學習時數 |
| ■ 銀行局電子支付機構內部稽核人員相關專業在職訓練時數 | ■ 上市上櫃公司董事、監察人進修時數 |

※ 歡迎企業包班，為您量身訂做所需課程。

※ 詳細課程規劃請上本會網站 www.caa.org.tw 查詢，或來電(02)2528-8875 洽詢。

電腦稽核期刊前期篇名整理

第三十九期_智慧金融環境下法令遵循與風險管理



- ◆ 金融 Chatbot 安全控管程序之探討
- ◆ FinTech 下遊戲產業洗錢風險與持續性稽核初探
- ◆ 財報不實民事損害賠償額計算之研究
- ◆ 淺論區塊鏈之發展與趨勢
- ◆ 舞弊稽核與鑑識會計對內部控制缺失之探討—以凱基銀行外匯交易損失為例

第三十八期_組織資料保護與利益關係人隱私



- ◆ 個人資料管理系統驗證要求事項標準化實施初論
- ◆ 大數據環境下政府審計之查核風險
- ◆ 外掛式資料查核及保護方案探討
- ◆ 醫療隱私之法律保障
- ◆ 以 MitmProxy 窺探手機應用程式隱私
- ◆ Location-based Privacy: Problems Analysis and Protection
- ◆ 歐盟 GDPR 與個人資料保護認證

訂購詳見電腦稽核協會網站<https://www.caa.org.tw/publish.php>

ISACA摘譯期刊近期篇名整理

第21期

2018年12月出刊



- ◆ 減少 IT 專案失敗的風險因子
Mitigating the Risk Factors of IT Project Failure
- ◆ 物聯網需要更好的安全性
IoT Needs Better Security
- ◆ 個資保護計畫的關鍵要素
Key Ingredients to Information Privacy Planning
- ◆ 以更少的資源做更多的事情
Doing More With Less
- ◆ 區塊鏈：辨識分散式分類帳的風險
Blockchain: Identifying Risk on the Road to Distributed Ledgers
- ◆ 解決產品應用面漏洞的共有性風險之評估方案
Addressing Shared Risk in Product Application Vulnerability Assessments

第22期

2019年06月出刊



- ◆ 企業大數據之審計
Auditing Big Data in Enterprises
- ◆ 運用人工智慧於應用程式安全
Applying AI in Application Security
- ◆ 機器學習稽核—CRISP-DM 架構
The Machine Learning Audit— CRISP-DM Framework
- ◆ 信息與通信審計之革新
Innovation in the IT Audit Process
- ◆ 資料隱私稽核
Auditing Data Privacy
- ◆ 區塊鏈技術的諾言和危險
The Promises and Jeopardies of Blockchain Technology

訂購詳見電腦稽核協會網站<https://www.caa.org.tw/publish.php>

近期活動報導

2019.01.07

1 月新竹例會

【新興資安風險議題與管理】

全球產業仰賴互聯網進行大量資料傳輸，資安事件逐漸受到重視，各國逐步訂定相關法規以避免重大災害出現。去年 10 月 Facebook 坦承被駭客竊取 2900 萬名用戶相關資料，而我國也曾發生因系統老舊，主機連線發生異常狀態，導致 ATM 跨行交易發生異常的狀況。除



◆ 1 月新竹例會 - 安侯企業管理股份有限公司數位科技安全部門邱述琛協理

此之外，資安攻擊更進一步利用 AI 技術進行惡意攻擊，測試其攻擊結果發現幾乎防不勝防。

本次月例會邀請安侯企業管理股份有限公司數位科技安全部門邱述琛協理以「新興資安風險議題與管理」為主題，從近期重大資安案例看資安風險趨勢，了解全球最新案例的脈絡，再以聯網設備網際安全發展現況，探討 IoT 風險管理管控，並介紹隱私工程與去識別化如何應用於組織中，最後介紹全球網際安全法規規範以及未來新興科技帶來的資訊安全管理挑戰。

1 月台北例會

2019.01.08

【從國際資訊服務管理標準改版看企業如何精進資訊服務品質及能量】

本次月例會邀請 BSI 英國標準協會台灣分公司謝君豪營運長以「從國際資訊服務管理標準改版看企業如何精進資訊服務品質及能量」為主題，分享資訊系統與服務流程優化的方法與重要性，並探討未來五年內 IoT 技術發展預估全球趨勢，以及數位化時代風險與機會並存，企業面臨何種關鍵挑戰，再以新創公司與上市櫃公司為比較解說董事會如何看待 IT 部門。最後介紹 ISO 20000 於 2018 年基於企業資訊部門服務應用改變而進行改版，改版後可從服務管理系統進行介入，提供服務時即可使用 ISO 20000。



◆ 1 月台北例會 - BSI 英國標準協會台灣分公司謝君豪營運長

協辦

2019.03.19

臺灣資安大會

2019 年臺灣資安大會以國際資安議題為主軸，舉辦為期三天的展覽及研討會、論壇，與 8000 名與會人共同分享討論資安各面向，相互交流分享最新知識與技術。

本次研討會邀請電腦稽核協會張紹斌理事長，以「從營業秘密的角度看資訊安全」為主題，分享營業秘密的法律概念以及資訊安全對營業秘密的重要性，資訊安全的涵蓋範圍較營業秘密廣，兩者之間又擁有直接或間接的關係，企業在面對問題發生時須考量多重因素後，判斷屬於資訊安全問題還是營業秘密問題。最後再分享實際案例並探討企業如何進行資訊安全佈局。



◆本會張紹斌理事長

2019.03.22

3 月台北例會

【行動應用資安之關鍵作法及防護要領】

隨行動裝置的普及化，工作或日常生活中經常大量使用行動裝置作為輔助，行動裝置已與生活密不可分。多數上架到 Android 市集的應用程式並未第三檢測或無嚴格規範，即便是規範較為嚴謹的 iOS store 也有一定的隱私洩漏風險。再加上大眾對於行動應裝置安全性問題較無警覺性，儼然形成巨大的危機。

此次例會邀請到行政院科技會報辦公室王仁甫研究員，以「行動應用資安之關鍵作法及防護要領」為主題，介紹美國資訊安全治理架構及解說資安是企業風險管理重要一環，再來分享未來行動化商業模式的風險及安全性，進而介紹我國行動化所面臨的關鍵問題，以及行動資安的發展，同時也分享世界各國行動資安產品的差異，最後以資安即國安政策為要點，分享行政院方案及落實資安旗艦計畫。



◆3 月台北例會 - 行政院科技會報辦公室王仁甫研究員

【運用 AI 與數據分析提升內部稽核作業】

AI 人工智慧的養成不可或缺的除了相應的技術外，最為重要的便是數據。正確、精準且大量的數據如同 AI 的糧食，供應 AI 成長為有助於企業應用的工具。大多數免費的公開資源對企業商業用途的幫助較少，企業所需的資源還是得仰賴平日長時間累積、整理數據所得，由此可知數據分析對於企業的重要性。

此次例會邀請到勤業眾信聯合會計師事務所風險諮詢曾韵執行副總經理及劉婉蓉副總經理，以「運用 AI 與數據分析提升內部稽核作業」為主題，由資料分析概論開始，介紹何謂大數據、大數據的資料來源以及常見的資料分析技術，如：資料探勘、社群網路分析、文字探勘等，而後介紹人工智能與資料分析趨勢，同時也分享 AI 可能帶來的風險。最後分享資料分析的實務應用，利用實際案例讓與會學員能更加瞭解資料分析的使用方法。



◆ 3月新竹例會-(左起)勤業眾信聯合會計師事務所風險諮詢曾韵執行副總經理及劉婉蓉副總經理

【企業如何從資訊服務落實資訊安全管理】

台灣整體產業對於資訊安全服務的需求逐日增加，可見各產業日漸重視資訊安全的重要性。而不同產業的資訊安全需求不同，對於提供資訊安全服務廠商來說，如何能確實有效提供服務是更為重要的一點。



◆ 4 月台北例會 - 台灣應用軟件股份有限公司葉顯榮總經理

此次例會邀請台灣應用軟件股份有限公司葉顯榮總經理，以「企業如何從資訊服務落實資訊安全管理」為主題，從「資訊安全管理」是防護也是服務為切入點，討論機房基礎設施、軟體發展維運服務環境、應用軟體維運等服務水準管理各項要點，再探討資訊安全管理與資訊服務管理的不同與應用，並從使用者觀點討論基於營運所需的管理系統，將所能提供的服務進行分類介紹，最後分享資訊安全管理服務成熟度等級的概念及改善方法，幫助學員能夠實際應用於職場中。

【遵循 ISO 20000 標準改善 IT 服務管理】

隨著現代科技高速發展演進，IT 產業除了技術上的成長外，也成功利用科學管理方式提升效率、控制風險與成本，逐漸轉型為精緻化的管理營運模式。無論對於 IT 內部營運組織或是 IT 服務外包公司來說，營運效率及服務都是至關重要的，故 ISO 20000 對於企業來說，是最好的 IT 服務管理認證。

此次例會邀請得安訊科技有限公司業務發展處吳安忠處長，以「遵循 ISO 20000 標準改善 IT 服務管理」為主題，從傳統 IT 產業管理模式開始進行探討其缺點，說明 IT 管理改革的緣起與目標；再來介紹 ISO 20000



◆ 5 月新竹例會 - 得安訊科技有限公司業務發展處吳安忠處長

的概念與架構，並介紹 2018 年 9 月發布之最新 ISO 20000-1:2018 標準，符合未來所有管理系統標準的高階結構。最後以實例解說 IT 服務改善的過程與成果，幫助學員了解如何做好 IT 服務管理以及未來趨勢走向。

2019.05.23

5月台北例會

【自動化威脅趨勢剖析與防禦對策】

由趨勢科技發表的 2019 資安年度預測報告中可見最新網路安全及攻擊趨勢，逐漸走向利用 AI 技術自動化且大量地進行資料竊取個人帳號密資料、試圖猜測密碼進行登入、網路釣魚等，並針對新興技術進行攻擊演進，令人防不勝防，極易造成巨大損失。



◆ 5月台北例會 - 星盾科技林育民技術長

此次例會邀請星盾科技林育民技術長以「自動化威脅趨勢剖析與防禦對策」為主題，從自動化威脅趨勢進行介紹、分析，分享從漏洞利用擬人化攻擊的各種新興案例，以及利用與生活密不可分的物聯網設備進行攻擊的原理及實際案例，並說明為何傳統安全機制無法有效保護物聯網設備的原因，對傳統安全機制所面臨的挑戰進行分析，最後介紹有效抵禦自動化威脅的方法，如教育訓練、動態幻象技術等，期望能將自動化威脅降到最低，提升資安效能。

北京市審計局參訪

2019.05.28

北京市審計局內部審計指導處李萬軍處長率北京市內部審計協會一行 15 人前來協會進行參訪交流，由本會黃秘書長代表接待，並簡報電腦稽核目前在台灣的發展與運用。



◆ 北京市審計局參訪參訪交流

2019 現代會計論壇學術研討會



◆ 6 月南區例會 - (左起) 雲林科技大學會計系孫嘉明助理教授、亞洲大學會計與資訊學系吳清在特聘教授、東海大學會計學系林秀鳳主任、亞洲大學會計與資訊學系周玲儀助理教授、勤業眾信聯合會計師事務所張益紳執行副總經理、資誠聯合會計師事務所張晉瑞執行董事、本會黃淙澤秘書長、本會張紹斌理事長、傑克自動化(股)公司黃秀鳳總經理、亞洲大學會計與資訊學系主任龐玉涓教授、亞洲大學會計與資訊學系歐進士講座教授、中華民國內部稽核協會劉振岩前理事長、國立中正大學黃士銘研發長、美國北伊利諾大學會計系李志真教授、逢甲大學會計學系盧鈺欣主任、國立中正大學會計與資訊科技學系黃劭彥副教授

因應人工智慧與巨量資料時代的來臨，培育具備富有前瞻宏觀、卓越創新之電腦稽核能力，已成為會計學界教育的重要目標。為切合產業需求培育人才，縮短學用落差，本研討會特針對外內部之審計稽核議題邀請產學專家參與指導與交流。

此次研討會分三場專題演講，第一場邀請亞洲大學林蔚君副校長分享「人工智慧驅動的數位轉型：機會與挑戰」，第二場邀請國立中正大學黃士銘研發長分享「AI 自動化技術將如何改變會計團隊的面貌」，第三場邀請美國北伊利諾大學會計系李志真教授分享「Embracing Change and Preparing Future Accountants」。而後進行會計實務座談，邀請勤業眾信聯合會計師事務所張益紳執行副總經理分享「從大數據稽核到全面風險智能儀表板」、安侯建業聯合會計師事務所陳怡如執行副總經理分享「邁向稽核與科技整合的新時代」、資誠聯合會計師事務所張晉瑞執行董事分享「預防性鑑識—以自駕車為例」以及安永聯合會計師事務所張騰龍執行副總經理分享「數位化時代對稽核的挑戰與機會」，最後由傑克自動化(股)公司黃秀鳳總經理分享「AI 人工智慧新稽核實務案例分享」，為所有與會學員帶來精采豐富的內容。

【 NIST Cybersecurity Framework 網路安全框架簡介 】

近年來因 IoT 興起，許多企業及公家單位開始使用 IoT 設備輔佐工作進行。2014 年，美國發生 3 起關鍵基礎設施遭受入侵事件，自此開始制定相關規範及標準，期望能減低類似狀況發生。NIST Cybersecurity Framework 網路安全框架在美國已有 30 個組織符合並採用，此標準是風險管理標準的概念，與組織現有的風險管理標準能夠契合在一起，可說是相容性高、易於使用的框架。

此次例會邀請 BSI 英國標準協會台灣分公司 NIST 花俊傑產品經理暨客戶經理以 NIST Cybersecurity Framework 網路安全框架簡介為主題，介紹網路安全框架發起的背景、框架的組成要素及應用，列出實施網路安全框架的七個步驟，讓企業組織能夠更加容易使用此框架。花經理也分享 NIST 官方網站可免費下載使用最新 1.1 版本，除此之外，ISACA 網站上會員也可下載 NIST 框架相關手冊，有簡體中文版，且有與 COBIT 結合的內容，提供給有需要的會員參考使用。



◆ 6 月台北例會 - BSI 英國標準協會台灣分公司 NIST 花俊傑產品經理暨客戶經理



證明您的能力足夠帶領企業面臨新時代的挑戰

資訊化是21世紀重要的時代特性，大量的資訊與相對應的技術支援，雖將能促進企業的成功，但在此環境下，卻同時也增加了許多原本沒有而複雜且具有挑戰性的新管理議題。

ISACA®國際電腦稽核協會是一個屬於世界領先地位的全球性組織，提供資訊專業人士能以卓越的途徑進行個人專業的成長與發展。同樣的，全球資訊專業人士也認為，ISACA對於他們的職業生涯發展與企業價值的提升均提供了實質的幫助。

將 CISA、CISM、CGEIT或CRISC的認證名稱放置在您名字後面，將能證明您的專業能力、經驗與推廣。這可認定您是一位專業的資訊人才，擁有全面性的資訊系統視野，並關係到企業能透過價值傳遞(value delivery)且獲得成功的關鍵因素。

隨著現代企業越來越依賴資訊系統(IS)，對於技術與資訊系統專業人員的需求快速的上升，並且更著重於資訊與治理的能力。企業需要合格的資訊專業人才的實務知識與專長，來幫助確認關鍵性問題與制定具體作法以支持資訊與相關技術的治理作為。ISACA的認證將滿足企業如此的迫切需求。ISACA以全球公認的認證讓企業能識別具備豐富經驗與知

在國際的獨立研究報告中指出，ISACA名稱代表著：

- 高階資訊專業人士的薪資報酬
- 可信賴的專業能力與認可
- 招募程序中的高點選率與優先面試

如何取得更多的資訊

訪問ISACA認證網站：www.isaca.org/certification-success

ISACA認證部門：certification@isaca.org



國際電腦稽核師(CISA)在稽核領域 如同註冊會計師(CPA)與公認會計師(CA)在會計領域一般



組織越來越依賴複雜的資訊作業來協助內部業務運作與控制措施的執行，企業需要擁有知識與技能的稽核專業人才，幫助企業找出關鍵問題與解決方案，以確認資訊系統的可信賴性與價值。

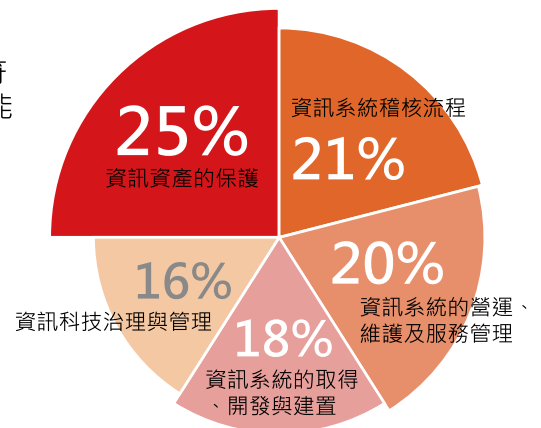
國際電腦稽核師證照(Certified Information Systems Auditor®, CISA®)是毋庸置疑的認證，當您擁有CISA證照，您的專業將立即得到理解與認同，CISA證照將讓您在國內與國際上對於使用標準、確認管理缺失、法規符合性，提供解決方案、發展控制措施以提供企業價值的專業知識、技能、經驗與可信賴的認可。

CISA認證是世界知名對於企業系統的稽核、控制、監控與資訊技術評估的標準。事實上在許多獨立的研究中指出，如資訊安全媒體集團(Information Security Media Group, ISMG)的每年就業趨勢調查，CISA始終是排名資訊證照中最搶手與薪資最高的認證。

歷經38年發展，現今CISA證照已是國際認可標準的具體實現，並且在162個國家有超過100,000位的專業人士獲得此項認證。

右表介紹CISA的專業工作活動項目，並指出每一專業領域的分配率。

CISA 專業領域考試範圍



證實您的資訊安全專業知識-提升競爭優勢



具備資訊安全管理專業人士的需求正呈現逐步上升的趨勢，國際資訊安全經理人(Certified Information Security Manager®, CISM®)是一項在資訊安全管理上全球公認的標準，現代企業必須保護自己免受網路犯罪與越來越多的惡意攻擊等問題，CISM以獨特並專注於資訊安全管理為著重點，提供資訊安全具體的實務做法。不同於其他的安全認證，CISM識別出個別的企業資訊安全管理、開發與佈建階段。

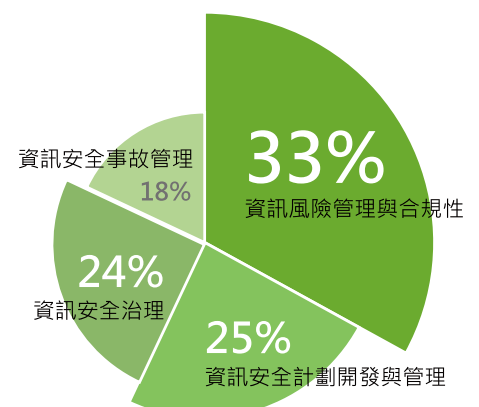
取得CISM的專業人士瞭解企業的需求，他們知道如何去管理和適應他們企業與行業的安全需求。CISM將不僅是具備資訊安全的專業知識，同時也在資訊安全的系統開發與管理上具有可靠的經驗。

CISM 驗證意涵著更高的收入潛力與職業發展。例如在最近的獨立研究2012年Foote Partners的資訊技能與證照報酬指數(IT Skills and Certifications Pay Index™, ITSCPI)中指出，CISM持續被列為高報酬與最受歡迎的資訊認證之一。

走過第13個年頭，目前已有超過21,300位專業人士取得CISM證照。

右表介紹CISM的專業工作活動項目，並指出每一專業領域的分配率。

CISM 專業領域考試範圍



展現您良好治理的能力 —對於您的企業與職業發展發揮廣大的影響力



避免發生意外(例如難以處理的資訊數據侵害)，對於企業來說是至關重要的，良好的治理將建立檢查與平衡機制，並對於發生意外事件能進行敏捷的反應。而當企業雇用了CGEIT，將可以確保具有良好的治理能力。

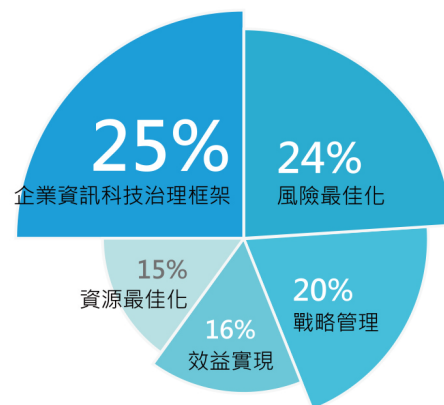
國際企業資訊治理師(Certified in the Governance of Enterprise IT®, CGEIT®)認可的專業人士具備對於企業資訊治理的原則與實踐有廣泛的知識與經驗。作為一位CGEIT的專業人士，您將證明您具有在一個組織中資訊治理的能力，由整體面掌握複雜的議題，並因此而提升對企業的价值。

CGEIT專業人士具備公認可信賴的資訊治理與策略定位等關鍵議題的知識與實務經驗，其所提供的公信力將使CGEIT的專業人士晉升成為「C-suite」高階經理人。

自2008年以來，已有超過5,000位專業人士取得CGEIT認證。

右表介紹CGEIT的專業工作活動項目，並指出每一專業領域的分配率。

CGEIT 專業領域考試範圍



個人事業與企業組織未來的試煉



對於改善公司治理、營運績效與安全基礎設施的需求不斷的增長，意味著資訊風險管理對於要能適應未來發展的企業是至關重要的。

國際資訊風險控制師(Certified in Risk and Information Systems Control™, CRISC™)是唯一針對資訊風險管理專業人士未來職業發展的驗證，其定位於有效連結資訊風險管理與企業風險管理，以成為企業戰略合作的夥伴。

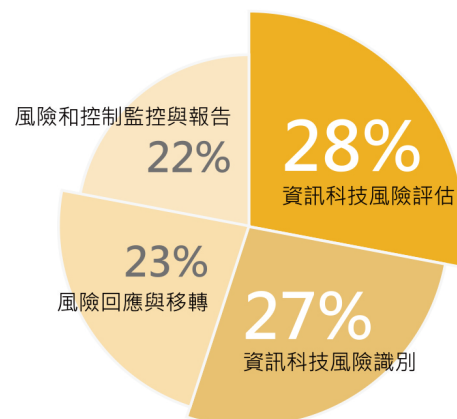
CRISC是最新且經過嚴格評核，具備識別資訊技術風險與評估資訊業務與風險管理的專業人士。CRISC證照將使您在企業內部資訊運作的未來發展上，提供更好的諮詢機會，並且使您在組織中的角色更顯重要；資訊風險將成為企業整體風險重要的組成部分，並使您在組織的資訊風險議題上成為知識型的領導者與內部規則變更的推動者。

2012年Foote Partners的資訊技能與證照報酬指數(IT Skills and Certifications Pay Index™, ITSCPI)，CRISC已擠身前10名薪資最高的認證之一。

自2010年以來，已有超過16,000位專業人士取得CRISC認證。

右表介紹CRISC的專業工作活動項目，並指出每一專業領域的分配率。

CRISC 專業領域考試範圍





CAA 電腦稽核



中華民國電腦稽核協會

11070台北市信義區基隆路一段143號7樓之4

7F.-4, No.143, Sec. 1, Keelung Rd., Xinyi Dist., Taipei City 11070, Taiwan (R.O.C.)

886-2-2528-8875 Fax : 886-2-2528-8876

www.caa.org.tw Web : www.isaca.org.tw