CAA 電腦稽核

Compliance and Risk Management in Smart Finance Environment

智慧金融環境下法令遵循與風險管理

Computer Audit Association

民國108年1月31日　第39期

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

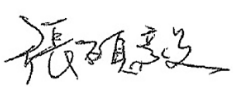
編 輯 序

近年來，隨著新經濟時代的崛起與智慧金融（Smart Finance）的快速發展，各國政府與企業積極的投入創新應用、轉型及擴大市場範圍，以滿足客戶在金融服務的需求。同時，金融服務之創新也為傳統金融業帶來許多變革，例如：行動支付、行動銀行、行動股票交易、貸款申請、投資理財、保險證券 … 等各項業務，都藉由與新興科技的結合來擴大產品和服務範圍；各式各樣創新應用如雨後春筍般地湧現，不斷挑戰金融生態系的現況。而在金融科技環境下，國際監理趨勢轉變、國內外與跨業競爭加劇、以及缺乏研發與創新投資等問題，都讓金融業面臨轉型的衝擊與競爭壓力。

此外，台灣資通訊技術發達，產業鏈完整，且有廣大中小企業可結合物聯網產業，參與發展社區智慧資源管理整合系統平台的建設商機。伴隨產生的金流需求，以智慧技術應用於數位金融服務創新，智慧金融的創新商業模式值得重視。資訊科技的創新發展也為金融業帶來許多監理新議題，國內外許多銀行因未能落實法令遵循制度，致使弊案層出不窮而導致重大損失，嚴重影響到投資大眾利益、社會安定及金融交易秩序。當金融科技發展日趨成熟之際，所有層級的風險控管必須更加以關注；尤其對於防制洗錢、打擊資恐、數位資訊安全、以及消費者權益保護等相關法令遵循案例，都是急於探討的重要議題。法令遵循制度已儼然成為金融業風險管理的重要一環，強化金融法令遵循之制度與功能、重視員工守法意識與維護企業形象，將可有效降低金融機構經營風險與責任。

綜上所述，電腦稽核期刊第三十九期以「智慧金融環境下法令遵循與風險管理」為主軸，由國內外學者與專家，提出具創新性與實用性的論文與新知。本期收錄文章內容理論和實務並重，包括：「金融 Chatbot 安全管控程序之探討」、「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之計算方式」、「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」、「使用 COBIT 進行資訊組織設計」、「COBIT 5 之風險架構：使 IT 風險管理變得有意義」、「運用 COBIT 5 評估資訊流程能力及對於世界彩券協會安全控制標準及 ISO 27001 之遵循程度」。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。

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。



編譯出版委員會主任委員
國立中正大學　管理學院院長

電腦稽核
COMPLIANCE AND RISK MANAGEMENT IN SMART FINANCE ENVIRONMENT
第 39 期

目 錄
CONTENTS

會務交流

發 行 人：張紹斌
總 編 輯：張碩毅
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
封面提字：林志雄
秘 書 長：黃淙澤
秘　　書：何慈雯、許秀玲、謝芷齡

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 2 樓之 2
電　　話：(02)2528-8875
網　　址：http://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 1 月 31 日
定　　價：新臺幣 250 元

金融Chatbot安全控管程序之探討

A Study of the Security Control Procedure of Banking Chatbot

賴森堂
實踐大學資訊科技與管理學系 助理教授
E-mail:stlai@mail.usc.edu.tw

摘　要

AI 再度興起，促使金融業務邁向智能化的金融科技 (FinTech)，具備 AI 技術的 Chatbot 則是擴展金融業務的重要成員之一，美國許多銀行及發卡公司已於 2017 年開始推出或導入聊天機器人，協助金融機構業務推動，以提升服務品質及市場競爭力。不過，AI 技術存在可能侵犯客戶資料與個人隱私的風險，使得安全性成為 Chatbot 必須重視的一項議題。為了提升 Chatbot 的安全性，本文剖析電子商務 (EC) 安全策略，並結合人工智慧 (AI) 安全原則，規劃一套 Chatbot 安全控管程序 (Chatbot Security Control Procedure，CSCP)，透過規範擬訂、規範遵循、活動檢視及改善作業等四個階段，監控金融 Chatbot 的安全狀況及識別 Chatbot 的安全缺失，適時協助改善安全措施，具體保護客戶資料安全與個人隱私。

關鍵詞：Chatbot、AI、EC、安全控管程序、FinTech

Abstract

The rise of AI has prompted the financial business to enter the intelligent financial technology (FinTech). Chatbot with AI technologies is an important tool of extension business. Many banks and card-issuing companies in the United States have introduced or launched Chatbots from 2017 to assist the business promotion, and improve conveniences, service quality and market competitiveness. However, the AI based Chatbot may infringe

on user privacy, which is a topic of concern. In order to monitor the security of banking Chatbot, this paper discusses EC security items and AI security limitations that affect banking Chatbot. Based on EC security strategy and AI security principles, the paper developed the Chatbot Security Control Procedure (CSCP). Monitoring Chatbot with CSCP can identify the security problems and defects of the banking Chatbot effectively. Banking Chatbot with high security precautions can reduce the user security risk. Using the CSCP to monitor the banking Chatbot activities can effectively protect the user data security and privacy.

Keywords: Chatbot, AI, CSCP, Privacy, Security

壹、前言

Chatbot 結合語言分析與語意剖析功能，是一項可以透過自然語言與人們交談或聊天的互動應用軟體，近年來許多實用的 Chatbot 陸續被推出，且積極融入人們日常生活中。Chatbot 目前大多用於協助電子商務 (Electronic Commerce，EC) 的相關服務 (Heo and Lee 2018)，如客戶服務中心、互聯網、金融理財洽詢等應用，這些用途的聊天機器人通常僅限於專門或特定領域的應用對話，並非針對人們之間的一般性交流與互動 (何維涓 2017)。1966 年，美國就已研發出世界第一套聊天機器人 (Güzeldere and Franchi 1995)，不過，當時受限於資訊設備效能不足且缺乏普及的網路環境，Chatbot 只能算是實驗室產品，並沒有實際應用於日常生活。近幾年，硬體設備與網路環境快速演進，AI 技術再度興起，促使 Chatbot 走出實驗室且大量投入商務應用。Gartner 的研究報告中預估，到了 2020 年，消費者與企業之間的互動模式將會由虛擬個人語音助理 (Virtual Personal Assistant，VPA) 為中心，串聯 App、API、Chatbot 等應用，能夠直接讓使用者透過語音指令與 Chatbot 互動 (Gartner 2018)。Makadia 報導指出：全球排名前 5 大銀行 (美國銀行、摩根大通、Capital One、萬事達卡及美國運通等) 都已導入 Chatbots (Makadia 2017) 。

客戶要求金融服務的過程，大多數需要與業務或專員面對面的交談，以獲得較完整的資訊與服務品質。不過，金融機構人力有限，客戶很難透過金融人員取得金融業務相關資訊與完善服務，非常缺乏便利性與互動機能。銀行業務與理財專員必須擁有財經的專業知識與多年經驗，甚至取得財務金融專業證照，才能勝任專業且繁瑣的金融業務。此外，業務與專員只能在特定時間內針對單一或特定客戶提供專業的服務，金融專業人員的服務方式就如同醫生看診一樣，無法在同一時間服務多位客戶。持續培養具專業知識及經驗的財經人員，成為金融機構拓展業務與開發客源的重要關鍵，而組織也必須付出可觀的訓練費用與人事成本。金融機構為有效提升客戶服務品質與市場競爭優勢，應積極邁向智能化 (Vieira and Sehgal 2018)。近年來，許多先進國家的金融機構

已開始導入或推出金融 Chatbot，協助或逐步取代銀行業務與理財專員的工作，可以獲得幾項實質的優勢，如有效降低人事成本、提高服務品質、結合 FinTech 的運作等，具體提升業者的市場競爭優勢。Grand view 研究報告指出，全球 Chatbot 市場將在 2025 年達到 12. 3 億美元產值，金融業更是積極導入 Chatbot 以提升市場競爭優勢 (Grand view 2017)。不過，涉及銀行與理財的業務，一般客戶只願意接受行員的服務，對於 AI 技術的金融 Chatbot，反而非一般客戶的首選，因此須提高金融 Chatbot 的信賴度與安全性才能增加客戶的使用意願。

金融 Chatbot 是具 AI 技術的商務軟體，可提供快速與便利的服務，不過，設計不當、濫用或隱含惡意程式的軟體，可能為客戶帶來無法預期的安全風險 (Letheren 2017)。為了強化金融 Chatbot 安全品質，本文以 EC 安全需求 (賴森堂 2002; Holcombe 2007) 與策略為基礎，參考 ASILOMAR 23 條人工智慧原則 (AI principles) (Future of life institute 2017) 與微軟 CEO 推動的「人工智慧安全六大守則」等相關安全機制 (Kawamoto 2016)，針對金融 Chatbot 規劃出一套 Chatbot 安全控管程序 (Chatbot Security Control Procedure，CSCP)，透過規範擬訂、規範遵循、活動檢視及改善作業等四個階段監測 Chatbot 的安全性，具體保護用戶資料安全與個人隱私。

貳、金融 Chatbot 與安全議題

具備 AI 特性的 Chatbot 是業務推動的重要利器，可具體提升金融機構的績效與競爭優勢。

一、金融 Chatbot 的現況

Borysowich 與 Bansal 2017 的研究 (Borysowich & Bansal 2017)，探討聊天機器人為銀行業帶來的變革，列出多項可為銀行業帶來的新機會，例如客戶服務、商品介紹、臨櫃服務、個人財務管理及財富管理等。國內許多銀行也都陸續導入 Chatbot，用來協助處理銀行相關業務，而目前的 Chatbot 著重於語言分析與語意剖析的能力，並未融入完整的 AI 技術，只適合擔任客服人員的助手，或是只處理或回答簡單的問題。黃彥綸碩士論文 (黃彥綸 2018) 評估與比較玉山銀行的「玉山小 i」Chatbot，與其他九家銀行 Chatbot 後，將「玉山小 i」歸屬於表現較佳的 Chatbot，然而有關 AI 技術，如知識能力、學習能力及連結能力都還有很多待成長的空間。因此，目前國內的金融 Chatbot 能夠處理的業務仍有限，多未涉及客戶財務與個人隱私，不過，當 AI 技術持續演進與成長，且業者以 Chatbot 取代金融專業人員為目標，將容許 Chatbot 可以存取、使用、搜集及推論客戶個人資料的權限，若完全沒有防範 AI 技術的安全機制，勢必衝擊客戶個人資料及隱私的安全風險。

二、金融理財 Chatbot 的業務與優勢

一般銀行業務員或理財專員通常須承辦且處理以下的業務：

1. 提供有關證券、債券、市場條件、投資前途及財務狀況等擬投資之資料。
2. 分析證券、債券、外匯及其他財務市場之趨勢。
3. 提供契約條款、股票及債券貸款之諮

詢及磋商，以便為客戶籌措資金。

4. 記錄及傳送證券、股票、公債、外匯等買賣訂單。

5. 開發新客戶。

6. 維護客戶關係。

7. 執行客戶指定之交易事項。

這些極為專業且繁瑣的工作需要具有多年經驗的承辦人員，且承辦人員須要花費較長時間完成一項理財服務，造成許多客戶無法取得適時的服務。此外金融服務內容涉及金流、客戶資料及個人隱私，銀行業務或理財專員必須建立良好的客戶關係，且取得客戶的高度信任，客戶才有意願提出理財的需求服務。

金融業為了克服人力資源的不足，又要維持服務品質，不得不朝數位化與智能化的方向演進，以金融 Chatbot 協助或取代銀行或理財專員的工作。舉如，萬事達卡與 Kasisto 合作推出人工智慧聊天機器人，從 2017 年初開始，美國地區的消費者可以利用 Chatbot 平台獲得銀行與金融的服務，服務內容包括：

1. 詢問個人帳戶資訊、
2. 查閱服務記錄、
3. 掌控個人花費、
4. 進一步瞭解萬事達卡持卡人權益、以及獲得金融理財的協助。

在 FinTech，各金融機構為了減輕人事費用、提升服務品質與市場競爭優勢，紛紛導入或推出可以協助甚至取代金融專業人員的金融 Chatbot。金融 Chatbot 是具有 AI 技術的應用軟體，因此不受服務時間及人數的限制，具學習能力、可調整性且訓練成本低等優勢。不過，如果安全性與可靠度不能獲得有效控管，對於客戶的錢財、資料與個人隱私，也可能相對帶來風險 (參閱表 1)。

表 1. 金融專業人員與 Chatbot 特性之比較

	金融專業人員	金融 Chatbot
可靠度	高	低
安全性	高	低
投入訓練成本	高	低
服務時間限制	受限	不受限
服務人數限制	受限	不受限
可調整性	低	高

* 本研究整理

三、AI 技術與安全風險

AI 應用軟體具備語意分析、推理、知識庫、主動搜尋及深度學習等多項能力 (Akerkar, and Sajja 2010；Vieira and Sehgal 2018)，這些 AI 技術採取便利的自然語言溝通方式，擁有持續擴增知識庫的知識，可以透過機器學習吸取多方面的經驗，如 Google AlphaGo 使用搜尋樹與深度學習等多種演算法，可像人類的大腦一樣自發學習進行直覺訓練，以提高下棋實力 (36Kr 2016)。AI 技術以網路主動搜尋能力帶動應用軟體持續的成長，強化應用軟體原有的功能，具有傳統應用軟體無法達到的效益與優勢。不過，一旦 AI 技術存在不當的設計、被濫用或隱含惡意程式，可能會形成難以預期的安全危機，危及用戶的資料安全與個人隱私。

EC 安全策略可以防範傳統電子商務系統違反資訊安全的行為，不過，Chatbot 具多項 AI 技術並非傳統電子商務系統，一旦未考量安全原則、缺乏透明性或出現異常狀況，可能會破壞 EC 安全策略，發生電腦犯罪行為 (Computer crime)，危害客戶個人資料與隱私 (簡立宗 2017；Stead 2018)。金融

Chatbot 融合多項 AI 技術，包括

1. 具有數據分析與知識推演能力，可以更瞭解客戶歸屬的投資類型，推薦更符合客戶需求的投資項目。
2. AI 可以從蒐集大量資料與多次互動的經驗中，學習且產生更完整的知識，以提升各項業務的推廣與處理能力。
3. 搜尋技術從網路的環境獲得客戶更多且更完整的資料，可能涉及客戶隱私。

如何防範 AI 應用軟體帶來的安全危機，2016 年以來，已有許多專家、學者與組織開始提出相關的論述，其中包括 Asilomar 23 條人工智慧原則 (Future of life institute 2017) 及微軟 CEO 推動的「人工智慧安全六大守則」(Kawamoto 2016)，顯示人們已經意識到 AI 發展可能引起的風險，從開發設計起點直接設定限制，讓日後的 AI 技術發展處於可控制的範圍 (Kawamoto 2016)。「Asilomar AI 原則」是開發安全 AI 的重要指南，已獲得 AI 社群與廣大從業者的廣泛支持 (Kawamoto 2016)。列舉其中 第 6 項及第 12 項如下：

1. 第 6 項 -- 安全性：人工智慧系統在它們整個的運轉週期內應該是安全可靠的，並且能在可應用的和可行的地方被驗證。
2. 第 12 項 -- 個人隱私：人們應該擁有權力去瀏覽、管理和控制他們產生的數據，考慮到人工智慧系統有分析和使用那些數據的能力。

微軟 CEO 於 2016 年建議人工智慧的研發要遵循六項原則 (Kawamoto 2016)，列舉其中第 2 項及第 4 項如下：

1. 第 2 項 AI 必須做到公開透明。
2. 第 4 項 AI 在設計的時候必須考慮到隱私保護。

另許多相關報導探討 AI 與隱私的議題中，台灣大學林守德教授表示，除了法律制度的保護之外，AI 涉及的隱私及安全在某種程度上，亦能透過技術來解決 (簡立宗 2017)。Julia Stead 認為消費者有權知道他們的個人資料是如何被 AI 所使用 (Stead 2018)，也就是 AI 必須做到公開透明。AI 開發的早期階段就應確保 AI 技術遵守個人資料保護權的規則 (DPA 2018)，這些都是使用 AI 技術的應用必須重視的項目。為了避免 Chatbot 利用 AI 技術危及客戶資料安全與個人隱私，如何有效管控 Chatbot 運作流程的安全性，成為金融 Chatbot 必須克服的一項重要挑戰。

參、Chatbot 應具備的安全考量

金融 Chatbot 是服務金融業務的聊天機器人，處理的業務涉及客戶財務與個人隱私，需要特別重視其安全性。

一、保護用戶資料安全與隱私的安全項目

金融 Chatbot 可以被視為具有 AI 特質的電子商務 (EC) 應用程式，因此，為了確保客戶的資料安全與個人隱私，金融 Chatbot 除了應考量安全需求 (賴森堂 2002；Holcombe 2007) 與身分驗證、授權、加密、審計等 EC 的安全措施 (Alin 2012)，還必須融入 AI 的安全原則 (參閱圖 1)，才能有效的建立 Chatbot 的安全防範機制，降低客戶個人資料與個人隱私的安全風險。EC

系統必須在開發前，就擬訂一套完善的安全需求，以強化系統的安全性。Holcombe認為電子商務必須滿足四項安全需求(Holcombe 2007)：

1. 授權(Authorization)：對於通過電子商務系統身分確證的使用者，必須授與該使用者系統功能的使用權限。
2. 完整性(Integrity)：在電子商務資料交換的過程中，必須確保資訊不會遭到任意的變更或篡改，以確定資訊內容的完整性。
3. 隱私性(Privacy)：在電子商務資料交換的過程中，必須避免未經授權人員的接觸及參與，以善加保護用戶的個人資料與交易資訊。
4. 不可否認性(Non-reputation)：各種電子商務的交易行為中，均能夠具體證明且記錄交易雙方都已經確實收到對方的交換資訊，以達到不可否認性。

至於EC安全措施除了融入四項安全需求，還必須訂定明確規範與稽核制度，EC安全措施包括：

1. 資料存取安全管制作業：
- 遵循資料存取權限，制定Chatbot資料存取規範。
- Chatbot 資料存取作業流程應採取log 機制，詳細記錄資料存取的步驟、內容及時間等細節，且融入異常資料存取的查核與檢視機制。
- 詳細記錄未遵循或違反資料存取權限的安全缺失。

2. 資料使用安全管制作業：
- 遵循資料使用權限，制定Chatbot資料使用規範。
- Chatbot 資料使用作業流程應採取log 機制，詳細記錄資料使用的步驟、內容及時間等細節，且融入異常資料使用的查核與檢視機制。
- 詳細記錄未遵循或違反資料使用權限的安全缺失。

3. 資料移轉(Transfer)安全管制作業：
- 遵循的資料交接權限，制定Chatbot資料移轉規範。
- Chatbot資料移轉作業流程應採取log機制，詳細記錄資料移轉的步驟、內容及時間等細節，且融入異常資料移轉的查核與檢視機制。
- 詳細記錄未遵循或違反資料移轉權限的安全缺失。

目前，AI技術的相關應用並沒有明確的安全規範與稽核制度，許多AI安全措施與制度都還在討論或研擬中，依據Chatbot的應用範疇與AI的技術特性，且參考討論中的AI原因，本文制定的AI安全限制作業包括：

1. 知識庫安全限制作業：知識可以透過學習與實務經驗不斷成長的，因此，對於知識庫涵蓋的內容應有明確的限制且必須受到嚴格監控，以避免不當的設計或濫用既有的知識竊取客戶的個人資料或侵犯客戶的隱私。
- 規範Chatbot 應遵循知識庫範圍限制。
- Chatbot 知識庫更動作業流程應採取log 機制，詳細記錄知識庫變動的步驟、內容及時間等細節，且融入知識庫的查核與檢視機制。
- 詳細記錄未遵循或違反知識庫範圍限制的安全缺失。

2. 機器學習安全限制作業：自主性的學習可能會破壞金融 Chatbot 應有規範與規矩。
- 規範 Chatbot 應遵循機器學習範圍限制。
- Chatbot 機器學習作業流程應採取 log 與透明機制，詳細記錄機器學習過程、步驟、及成效等細節，且融入學習成效的查核與檢視機制。
- 詳細記錄未遵循或違反機器學習範圍限制的安全缺失。

3. 資訊搜尋安全限制作業：擴展業務、開發新客是金融 Chatbot 的工作任務，應避免 Chatbot 為了開發新客，而以客戶名義進行不當的資訊搜尋，侵犯客戶隱私。
- 規範 Chatbot 應遵循資訊搜尋範圍限制。
- Chatbot 資訊搜尋作業流程應採取 log 與透明機制，詳細記錄資訊搜尋的活動、步驟、範圍及時間等細節，且融入搜尋作業的查核與檢視機制。
- 詳細記錄未遵循或違反資訊搜尋範圍限制的安全缺失。

最後，從 AI 安全原則切入，為了防範 AI 的設計不當與惡意程式造成客戶的安全風險，還必須注重金融 Chatbot 的高度透明性，確保 Chatbot 具備可以隨時被檢視與調整的空間。

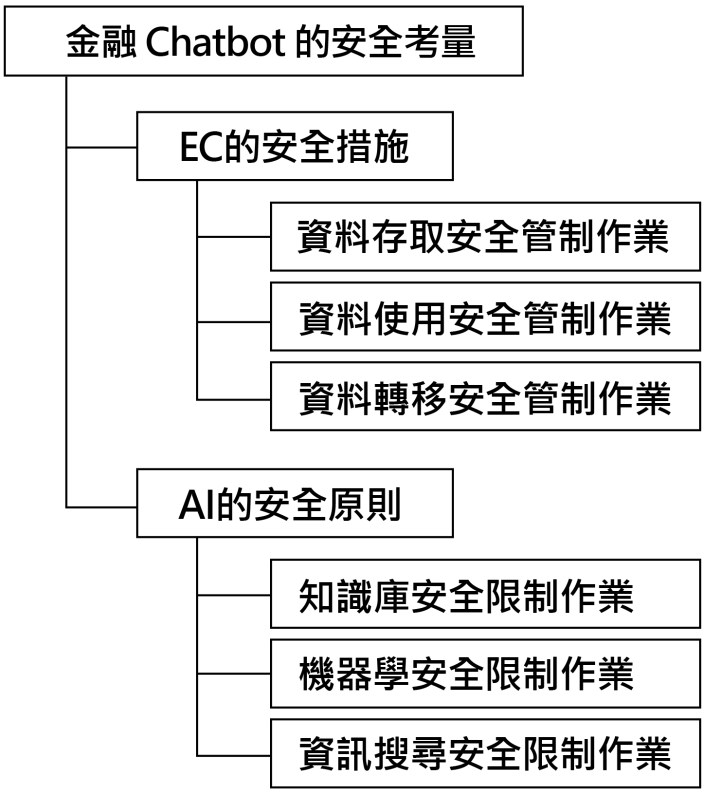


圖 1. 兩層式安全防範架構圖（本研究整理）

二、安全項目之檢測方式

具有 AI 技術的 Chatbot 應用軟體除了擬訂安全的防範規範外，必須融入公開透明的特質，可以隨時接受稽核人員的檢視活動，維運人員的調整與改善作業，高度的安全防範措施，可以避免給用戶帶來安全風險。

1. 資料存取安全
- 應擬訂 Chatbot 資料存取權限規範、
- 應遵循 Chatbot 資料存取權限規範進行開發設計流程、
- Chatbot 應融入透明性，協助資料存取權限的檢視活動。

2. 資料使用安全
- 應擬訂 Chatbot 資料使用權限規範、
- 應遵循 Chatbot 資料使用權限規範進行開發設計流程、
- Chatbot 應融入透明性，協助資料使用權限的檢視活動。

3. 資料移轉安全
- 應擬訂 Chatbot 資料移轉權限規範、
- 應遵循 Chatbot 資料移轉權限規範進行開發設計流程、
- Chatbot 應融入透明性，協助資料移轉權限的檢視活動。

4. 知識庫安全限制
- 應擬訂 Chatbot 知識庫安全限制規範、
- 應遵循 Chatbot 知識庫安全限制規範進行設計開發流程、
- Chatbot 應融入透明性，協助知識庫安全限制的檢視活動。

5. 機器學習安全限制
- 應擬訂 Chatbot 機器學習安全限制規範、
- 應遵循 Chatbot 機器學習安全限制規範進行開發設計開發流程、
- Chatbot 應融入透明性，協助機器學習安全限制的檢視活動。

6. 資訊搜尋安全限制
- 應擬訂 Chatbot 資訊搜尋安全限制規範、
- 應遵循 Chatbot 資訊搜尋安全限制範圍規範進行設計開發流程、
- Chatbot 應融入透明性，協助資訊搜尋安全限制的檢視活動。

肆、Chatbot 安全控管程序與效益評估

為確保金融 Chatbot 具備應有的安全性與可靠度，在設計與運作過程中，必須制定相關的規範與檢視活動。

一、持續性的安全控管程序

為了保障客戶的資料安全與個人隱私，本文以 EC 的安全措施為基礎再結合 AI 的安全原則，規劃出一套 Chatbot 安全控管程序 (CSCP)，CSCP 依 PDCA 流程設計規範擬訂、規範遵循、活動監測及改善措施等四個階段性作業 (參閱圖 2)，說明如下：

1. 前置作業階段：本階段包含三個工作項，
- 首先，擬 (修) 訂完整、嚴謹且符合 EC 安全措施的資料存取、資料使用與資料移轉等安全規範。接著，擬訂完整、可靠且符合 AI 安全原則的知識庫、機器學習與資訊搜尋等安全限制規範。

・審核 EC 安全規範與 AI 安全限制：
- 審核「Chatbot 資料存取管制」規範已確實依 EC 安全措施擬訂。
- 審核「Chatbot 資料使用管制」規範已確實依 EC 安全措施擬訂。
- 審核「Chatbot 資料移轉管制」規範已確實依 EC 安全措施擬訂。
- 審核「Chatbot 知識庫限制」規範已確實依 AI 安全原則擬訂。
- 審核「Chatbot 機器學習限制」規範已確實依 AI 安全原則擬訂。
- 審核「Chatbot 資訊搜尋限制」規範已確實依 AI 安全原則擬訂。

・未通過審核之 EC 安全規範與 AI 安全限制：
- 若發現 EC 安全規範存在不完整、不一致或不正確的內容，須退回前項工作進行修訂且重新審核。
- 若發現 AI 限制規範存在不完整、不一致或不正確的內容，須退回前項工作進行修訂且重新審核。

2. 設計實作階段：本階段檢視金融 Chatbot 設計開發是否確實遵循 EC 安全規範與 AI 安全限制。一旦發現未遵循規範或有安全缺失，須詳細記錄缺失項目與內容，以供後續改善作業。

・先確認 Chatbot 設計開發已遵循 EC 安全規範，再確認 Chatbot 設計開發已遵循 AI 安全限制。

・若發現未遵循 EC 安全規範或 AI 安全限制的設計實作內容，應詳細記錄安全缺失的項目與內容。

・設計實作階段審查應依據遵循作業存在問題與缺失的嚴重性，裁決退回修正或待後續改善。

3. 持續監測階段：本階段為確保金融 Chatbot 都能在正常且安全的狀態下運作，應採取持續監控金融 Chatbot 運作流程是否都符合 EC 安全規範與 AI 限制規範。一旦發現未遵循規範或有安全缺失，須詳細記錄未遵循項目與缺失內容，以供後續改善作業。

・以 log 日誌機制，監控 Chatbot 運作流程確認符合 EC 安全規範。

・以透明性機制，監控 Chatbot 運作流程確認符合 AI 限制規範。

・一旦發現未遵循規範或有安全缺失，須詳細記錄未遵循項目與缺失內容，以供後續改善作業。

・持續監測階段審查應依據運作流程問題與缺失的嚴重性，裁決退回修正或待後續改善。

4. 缺失改善階段：本階段依據安全缺失記錄，找出安全缺失違反規範或限制之狀況與原因，再針對安全缺失狀況與原因提出安全改善措施。

・從缺失記錄找出安全缺失之狀況與原因，再依 EC 安全規範或 AI 安全限制提出安全缺失改善措施。

・確認依 EC 安全規範或 AI 安全缺失改善措施完成改善作業。

・缺失改善階段審查應改善作業成效與達成率，裁決退回重做或有條件改善。

二、Chatbot 的效益評估

一般接受金融服務的客戶族群除了注重快速且便利的服務品質外，最在意的還是資料安全、個人隱私與可靠度的議題，因為缺乏安全性的服務內容，將很難取得客戶的信賴更無法擴展客源，因而導致客戶族群的流失且喪失市場競爭力。本文剖析 EC 安全策略，且結合 AI 安全原則，擬訂出一套 CSCP，用以強化金融 Chatbot 的安全性，使得客戶在享有便利性與高品質的金融服務外，還能保有高安全性的服務內容，有效保護客戶資料安全與個人隱私。金融 Chatbot 可以為金融機構帶來的多項商機與效益，CSCP 的五大優勢更可提升金融 Chatbot 的安全品質，說明如下：

- 結合 EC 安全策略：金融 Chatbot 是屬於一項金融服務的商務軟體，因此，金融 Chatbot 必須考量 EC 運作所擬訂的安全策略，以防範金融服務的安全漏洞與缺失。

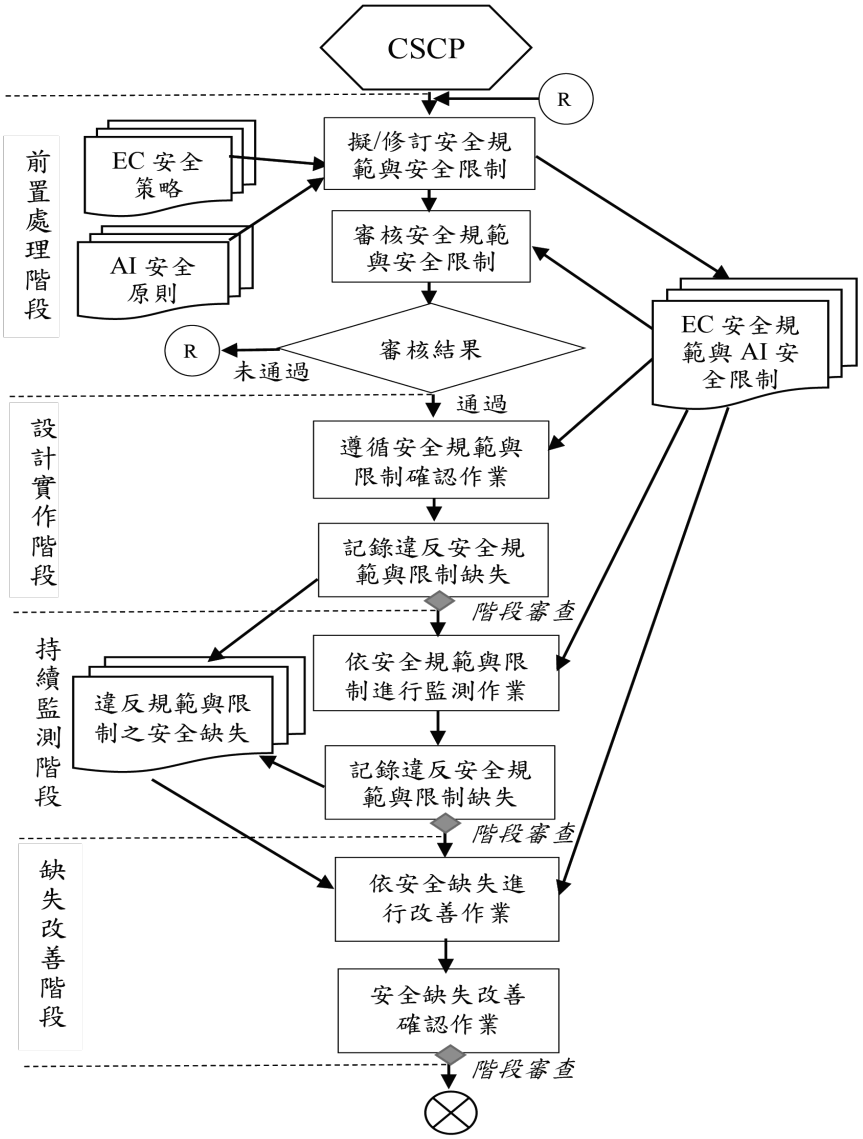


圖 2. CSCP 的運作流程圖（本研究整理）

- 融入 AI 安全原則：Chatbot 是 AI 的應用軟體，AI 技術設計不當或遭到濫用，可能會造成用戶無法預期安全風險，金融 Chatbot 必須考量 AI 運作可能出現的安全問題，以 AI 安全原則融入金融 Chatbot 的 AI 安全防範機制，可以降低 AI 技術上的安全風險。
- 具透明性的檢視活動：嚴格要求金融 Chatbot 必須採取 Log 機制，確實記錄關鍵或異常活動內容，同時在重要的查核點必須嵌入可監測的功能，利用追溯與檢視活動識別作業的安全缺失。
- 協助識別安全缺失：CSCP 以規範擬訂、規範遵循、活動檢視及改善作業等四個階段協助識別、記錄且改善金融 Chatbot 的安全缺失。
- 強調改善機制：依據金融 Chatbot 的安全缺失記錄，提出具體的改善措施，以適時彌補 Chatbot 的安全缺失與漏洞。

以金融 Chatbot 採用 CSCP 的安全控管程序與無任何安全控管程序的差異，可以突顯 CSCP 結合 EC 的安全策略、融入 AI 的安全原則、具透明性的檢視活動、協助識別安全缺失及強調改善機制等優勢 (參閱表 2)。

表 2. CSCP 關鍵項目評估表

有無使用 CSCP 安全關鍵項目	使用 CSCP 的金融 Chatbot	無安全控管的金融 Chatbot
結合 EC 的安全策略	V	V
融入 AI 的安全原則	V	-
具透明性的檢視活動	V	-
協助識別安全缺失	V	-
強調改善機制	V	-

* 本研究整理

伍、結論

金融 Chatbot 是 FinTech 的主要成員之一，結合 AI 的多項技術，Chatbot 可以協助或逐漸取代銀行業務與理財專員的工作，除了可大幅降低金融業人事成本外，更可以開發新客戶、提高工作效益與服務品質。不過，對於接受金融服務的客戶而言，信賴度、資料的安全與個人隱私才是關注的議題，Chatbot 擁有多項 AI 技術，一旦設計不當、被濫用或存在惡意的程式，都可能為客戶給帶來難以預期的安全風險。為了保護客戶資料安全與個人隱私，本文以 EC 安全策略基礎且同時考量 AI 安全原則，規劃一套 Chatbot 安全控管程序 (CSCP)。使用 CSCP 監控 Chatbot，可以在特定的階段適時識別金融 Chatbot 的安全問題與缺失。金融 Chatbot 持有高安全性的防範措施可以有效降低客戶的安全風險，使用 CSCP 監控金融 Chatbot 安全性，可以有效保護客戶資料安全與個人隱私。本文擬訂的 CSCP 以四個作業階段管控金融 Chatbot 安全性，CSCP 主要的貢獻如下：

- 以 EC 安全策略結合 AI 安全原則制定安全防範規範。
- 要求 Chatbot 必須遵循 EC 與 AI 安全規範。
- 採取持續的監控措施，有效識別安全缺失。
- 具體保護客戶資料安全與個人隱私。

參考文獻

1. 何維涓，2017，Chatbot 成 2017 年企業熱門應用，iThome, http://www.ithome.com.tw/news/ 115586

2. 賴森堂 ，2002，電子商務軟體品質量測模式，企業管理學報，第 53 期，53- 72 頁，國立臺北大學企業管理學系。

3. 黃彥綸，2018，ChatBot 運作品質與效益改善方法之研究，實踐大學資訊科技與管理學系碩士班碩士學位論文。

4. 簡立宗，2017，資料保護、安全隱私 AI 發展最基礎課題，工商時報 (http://www.chinatimes.com/newspapers/ 20171011000154- 260210)

5. 36Kr，2016，深入淺出，解讀 Google 的人工智慧圍棋「大腦」，數位時代 .

6.Heo, M., & Lee, K. J., 2018, Chatbot as a New Business Communication Tool: The Case of Naver TalkTalk. Business Communication Research and Practice, 1(1), 41- 45.

7. Güzeldere, Güven and Franchi, Stefano, 1995, Constructions of the Mind, Stanford Humanities Review, SEHR, Stanford University, 4 (2)

8. Gartner, 2018, Gartner Says 25 Percent of Customer Service Operations Will Use Virtual Customer Assistants by 2020, TOKYO, Japan. (https://www.gartner.com/en/newsroom/press-releases/ 2018-02- 19-gartner-says- 25-percent-of-customer-service-operations-will-use-virtual-customer-assistants-by- 2020)

9. Grand View Research, 2017, Chatbot Market Size To Reach $ 1. 25 Billion By 2025, (https://www.grandviewresearch.com/press-release/global-Chatbot-market)

10. Makadia, Mitul, 2017, Chatbots in Banking: Which Are the Top 5 Banks That Have Adopted Chatbots? ,Infographic September 22. https://www.business 2community.com/infographics/Chatbots-banking-top- 5-banks-adopted-Chatbots-infographic- 01917176

11. Vieira, A., & Sehgal, A., 2018, How Banks Can Better Serve Their Customers Through Artificial Techniques. In Digital Marketplaces Unleashed, Springer, Berlin, Heidelberg, pp. 311- 326

12. Letheren, K., & Dootson, P., 2017, Banking with a Chatbot: A Battle between convenience and security. The Conversation.

13. Holcombe, C., 2007, Advanced Guide to eCommerce, LitLangs Publishing, 2007.

14. Future of Life Institute, 2017, ASILOMAR AI PRINCIPLES, 2017 Asilomar conference https://futureoflife.org/ai-principles/

15. Borysowich, C. and Bansal, S. 2017, FINANCIAL CHATBOTS A LANDSCAPE OF WHITE LABEL BANKING PRODUCTS, The Capital Markets Company, pp. 2- 21.

16. Alin, M., 2012, E-COMMERCE SECURITY STRATEGIES. STATISTICS AND ECONOMIC INFORMATICS, 375. Journal of Internet Banking and Commerce, vol. 17, no. 3

17. Akerkar, R., & Sajja, P., 2010, Knowledge-based systems. Jones & Bartlett Publishers.

18. Stead, Julia, 2018, How to Address Consumer AI Privacy Concerns, CMSWIRE. https://www.cmswire.com/customer-experience/how-to-address-consumer-ai-privacy-concerns/

19. The Norwegian Data Protection Authority (DPA), 2018, Artificial intelligence and privacy. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

20. Kawamoto, D., 2016, Microsoft's Satya Nadella: 6 Must-Have AI Design Principles, informationWeek,. https://www.informationweek.com/cloud/microsofts-satya-nadella- 6-must-have-ai-design-principles/d/d-id/ 1326109

FinTech下遊戲產業洗錢風險與持續性稽核初探

Continuously Computer Auditing Program of Money Laundering Risk on Video Game Industry under FinTech Environment

賴虹霖
致理科技大學會計資訊系 副教授
mail:debbielai@mail.chihlee.edu.tw

李岱芸、余佳臻、郭紘志、楊雅晴、簡嘉妤、饒庭瑜
致理科技大學會計資訊系 學生
mail:10411329@mail.chihlee.edu.tw

摘　要

隨著科技的進步，金融科技在各個產業中都開始扮演重要的角色。而遊戲產業是近年來發展快速的行業，電競產業的興盛及體育化為遊戲產業帶來了巨大的收益，然而在遊戲產業和電子商務的蓬勃發展之下，也會帶來許多隱藏的風險，其中也包括了透過金融科技所衍生的風險，特別是在國際間非常重要的洗錢風險。

因此，為了避免遊戲產業成為不肖人士洗錢的途徑，故本研究利用持續性稽核的功能，針對遊戲業者之內部控制及調查業者常發生之作業問題，透過電腦稽核軟體提出有效的輔助管理稽核報表，以協助業者及早發現問題，避免出現被利用為洗錢途徑之風險。

本研究透過深度訪談及實際觀察後，利用模擬資料做出二個持續性稽核測試程式：超商點數銷售之高風險分店測試、退款交易安全性測試，透過所設計之稽核程式，能夠自動即時偵測出異常交易或異常帳號，並進一步追蹤後續。

關鍵詞：洗錢風險、持續性稽核、遊戲產業、電腦輔助稽核

Abstract

With the evolution of information technology on the Internet, Financial Technology (FinTech) is playing an important role in each industry. Nowadays, with the rapid development of video game industry, it brings lots of revenues but also risks the industry. One of the risks is derived from FinTech, such as money laundering risk.

In order to avoid money laundering risk in video game industry, the study uses continuous audit function to help with their internal control and operational issues. Through the computer audit software, effective supplementary management audit report can be generated to help the company to identify issues at an early stage before it gets into troubles.

This study uses simulation data to make the following two continuous audit test programs to detect automatically whether the internal control of the video game industry is problematic: the high risk store, the security of reimbursement.

Keywords：Money laundering risk, Continuously auditing, Video game industry, Computer-assisted audit.

壹、緒論

一、研究動機

線上遊戲一直是人們休閒娛樂的選擇之一，隨著科技進步因此發展了多元的遊戲種類，也帶動了遊戲產業發展。全球遊戲市場一直是穩定成長，2015 年因電競產業興起而大幅增長，2017 年更是比 2016 年成長了近一成，電競產業的興盛及體育化為遊戲產業帶來了巨大的收益，全球最大的遊戲分析公司 Newzoo 於 2017 年底提出的遊戲市場報告中表示不論是線上遊戲、手機遊戲、主機遊戲等在未來都將有更大幅度的提高。

而根據工商時報 2017 年報導，2016 年台灣遊戲市場收入已達 510 億台幣，市場前景看好，加上正式將電競賽事納入運動

產業，預估 2021 年台灣遊戲市場收入更可能上看 690 億台幣，台灣電競產業發展蓬勃指日可待。(工商時報 2017 年 12 月 25 日)。

值此之時，在商業模式推陳出新下，網際網路的普及和電子商務的蓬勃發展，支付方式也有了多元化的發展，第三方支付服務應運而生。(中央社新聞 2017 年 12 月 26 日) 而隨著科技的日新月異與科技始終來自於人性的理念，「 金融科技 」也因此產生並開始成為潮流。

「 金融科技 」Financial technology (又稱 FinTech)，是利用科技手段讓企業在金融服務方面更加有效率。因此，任何與金融有關的科技都可以被稱為金融科技 (張中一 2016 年)。

2015 年台灣金管會開始大動作開放銀行投資 FinTech，首要推動臺灣電子支付比率 5 年倍增計畫，通過電子支付取代傳統的貨幣流通，不僅能大幅減少攜帶大筆現金可能遭搶的風險並且能有效杜絕假幣氾濫，雖然電子支付確實能有效解決傳統支付存在的風險問題，但卻也衍生了新的風險，其中包括惡意詐騙、技術漏洞、駭客攻擊和技術詐騙等，已然成為電子支付下不可避免的風險。(人民日報 2017 年 07 月 07 日)

隨著網際網路的發展普及，資訊的串聯跨越了國境、人種、語言等，為人類帶來了更快速的資訊傳遞，但同時也有人利用其隱密性高及傳播速度快之特性，從事不法行為，因而產生與傳統犯罪不同的新型態犯罪。(內政部警政署 2017 年 03 月 08 日)。根據內政部警政署資料 (2017 年) 得知，使用電腦網路犯罪主要以「 詐欺 」最多，2016 年明顯較 2015 年大幅上漲，2017 年雖小幅下降但仍維持在一定數量，居高不下。

遊戲市場商機大，詐騙集團常利用遊戲頻道販售低於市場價格的虛擬寶物，以此吸引買家以匯款方式付款，等買家匯款完成卻遲遲等不到賣家蹤影，因此，警方及遊戲公司呼籲民眾提高警覺，購買遊戲虛擬物品等，透過官方網站較能獲得保障。(蘋果日報 2017 年 07 月 01 日)

二、研究目的及範圍

基於前述背景及案例，得知在遊戲產業和電子商務的蓬勃發展之下，將會帶來許多隱藏風險。而稽核的功能發揮，則有助於健全組織之內部制度並強化公司治理之監督機制。(蘇裕惠 2006 年)

本研究是針對有關於台灣遊戲產業業者內部控制的了解，調查近年來金融科技的衝擊對台灣遊戲產業業者的影響並分析其風險，利用電腦稽核軟體針對我國遊戲業的內部控制提出有效的輔助管理稽核報表，以協助業者及早發現問題避免經營上出現困難。

本研究透過深度訪談了解遊戲公司作業流程，以設計出持續性稽核作業來協助遊戲業者，但每家遊戲公司狀況不同，所以不一定適用於所有遊戲公司。

三、研究架構

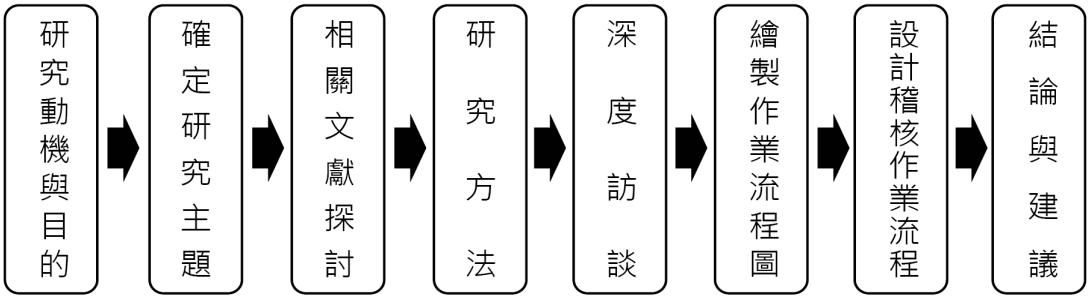


圖 1 研究架構

貳、文獻探討

2017 年可以說是遊戲產業重要的一年，全球遊戲玩家達 22 億人較 2016 年成長了 5%，全球遊戲市場從 2016 年的 996 億美元攀升至 1160 億美元。國際奧林匹克委員會（International Olympic Committee，IOC）、亞洲奧林匹克理事會（The Olympic Counsil of Asia，OCA）都相繼認可電競為運動產業的一種，更將於 2024 年巴黎奧運成為正式比賽項目。(蘋果日報 2017 年 11 月 10 日 ）

在遊戲產業蓬勃發展之下，背後卻也隱藏了無數的危害及風險，對遊戲業者的內部風險來說，面臨的問題也隨之出現，從遊戲設計的程式漏洞、遊戲性質相似度高，導致遊戲生命週期縮短等，從外部風險來說，近年來金融科技的發展為人們金錢流通帶來了便捷的使用，許多遊戲廠商亦看準這塊商機紛紛投入，卻也帶來了更多的風險問題，像是資訊安全、洗錢防制等。

在遊戲產業的蓬勃發展以及科技方面的進步，導致越來越多企業透過金融科技的方式來進行交易，然而在遊戲產業的快速發展之下，如何因應風險也成為一個重要的問題。以下將針對金融科技方面做進一步的介紹。

一、金融科技之延伸

金融科技是指運用科技讓金融服務變得更加快速，包含了支付、融資、投資等。其中被極力推廣的行動支付，是指可透過連網的行動裝置，取代實體信用卡、票卡或現金進行交易行為，而行動支付可分為電子支付及第三方支付。以下將介紹與金融科技息息相關的支付方面。

遊戲業是一個虛擬社會，進入遊戲前會需要玩家註冊會員，才能進行遊戲點數的購買，遊戲業者管理遊戲玩家的帳號不可重複，也管理每個帳號下所有的交易記錄及所儲值的點數，相對的資訊安全顯得重要。

依遊戲商的分析，遊戲產業的資源包括遊戲會員平台，還有可靠性高的遊戲點數儲值系統，讓玩家消費及儲值點數時能減少阻礙。而這些資源也就是遊戲業潛在的優勢，擁有大量遊戲會員且都有購買點數儲值的這些電子支付的交易經驗，也有與銀行、超商等通路購買的經驗。因此在推動電子支付時，比其他產業的業者更具優勢。(柳哲豪 2017 年 ）

二、第三方支付風險因子

吳淑娟（2015 年 ）的研究中指出，第三方支付的風險因子包含交易安全、資訊安全、資產保全、駭客攻擊、法規風險。

根據上述提出的第三方支付風險會衍生出的相關問題，如：若沒有應對機制來追查資金往來，容易造成洗錢問題，另外網路帶來便利的同時也必須防範駭客入侵的資安問題，本研究將在以下會有更深入的說明。

（一）洗錢風險

1. 洗錢定義

洗錢係指從事不法活動或非法交易之人，將來源不明的資金透過金融或非金融機構等仲介機構之運作，經過金融機構的合法金錢循環系統後，將黑錢漂淨，掩飾其不法資金來源之本質，藉以規避法律追查之行為這過程稱之洗錢。新洗錢防制法 106 年 6 月 28 日上路，新法修正重點：1. 降低洗錢犯罪率 2. 金流透明化 3. 強化洗錢防制體系 4. 接軌國際規範。（許義寶 2012 年 ）

2. 洗錢之過程

國際金融反洗錢特別工作小組（ Financial Action Task Force on money laundering，簡稱 FATF）將洗錢過程區分以下三個階段：（張孟妍 2017 年 ）

（1）存放：為洗錢活動的第一個步驟，主要目的是將大量現金混入合法金錢循環系統中，利用不同銀行間相互轉存，透過虛偽的帳目移轉，能更有效地逃脫司法機關之偵查，達到掩飾其非法目的。

（2）多層化：利用金融機構設立人頭帳戶，透過電匯方式，或者將不法所得轉換成不動產、期貨、有價證券等財物，導入金融或非金融體系中，藉由許多複雜金融交易來掩飾犯罪所得。

（3）整合：經過多層化階段，使用不同的資金轉換掩飾後，將最後被清洗的資金移入於合法資金中，以切斷與非法資金之關聯性，洗錢犯罪者得以自由運作，將清洗後的財產如合法財產般融入經濟體系，為洗錢犯罪者之最終目的。

因近期大量發展金融科技，眾多業者也將交易方式轉向第三方支付，但臺灣對於第三方支付相關法規並未制定完善，因此洗錢犯罪者可能藉此漏洞，利用第三方支付洗錢。

（二）新洗錢型態

猴集仁（2012 年）指出隨著網路科技快速發展，促進全球經濟發展，同時，犯罪者利用網路銀行或者新支付系統進行金融交易，從事洗錢活動。網路銀行為新洗錢型態，客戶無須親自到金融機構櫃檯辦理，金融機構及客戶間僅透過網路銀行，即可直接取得金融機構提供的服務。洗錢防制法對傳統金融機構的規範日益完善，透過傳統金融機構洗錢將是屬於高風險低報酬之處置，不符合洗錢犯罪者為確保其非法所得之目的，加上近期網路銀行、第三

方支付方式逐漸興起，更具隱密、不易辨識、難以追蹤之特性，故洗錢犯罪者可能轉向利用「新興支付方式」完成洗錢活動。

（三）洗錢案例

1. P 2P 網絡借貸潛在的非法集資

P 2P 作為線上電子支付互聯網的一種形態，一方面進入門檻低，需求者眾多，另一方面犯罪者應用 P 2P 的貸款購買不動產或貴重物品等，洗錢犯罪者正利用傳統或非傳統金融機構隱匿犯罪所得來源。我國的 P 2P 公司，金管會尚未將此線上交易活動納入反洗錢監管框架內，因此 P 2P 網絡借貸常被犯罪者用來洗錢管道。（中國證券報 2016 年 12 月 07 日）

2. 虛擬貨幣 G 幣

在法務部調查局 2016 年報中提出，「 MCLUB」網站係國外 M 集團旗下虛擬貨幣 G（下稱 G 幣）之遊戲代幣平臺，投資人將投資款項以現金交付或匯款至旗下分公司指定帳戶，並於「 MCLUB」網站註冊後，即可完成投資，取得 G 幣之電子交易帳號。該網站並依投資配套，提撥一定數量之 G 幣至投資人帳戶，投資人即可使用 G 幣。G 幣採分批方式銷售，每批數量及初始價格均由 M 集團決定，並隨銷售數量增加而逐步抬高價格，俟該批 G 幣總量銷售完畢後，M 集團擇定 G 幣拆分時間倍數，拆分後 G 幣價格回跌（仍高於起始價格），原投資人持有之 G 幣數量則倍增。

M 集團利用網路平台操作投資、贖回等手續，吸引投資人加入，且提供實體商品、電子票證及有價證券做為贖回標的，外表看似投資結構更為複雜，但其本質，仍與保證贖回本金及給付與顯不相當之獲利的傳統吸金手法並無二致，電子票證或電子支付等虛擬貨幣已成為新興犯罪工具。

如同前述，遊戲產業與金融科技之結合，可能衍生相關風險，故本研究將從遊戲買賣流程面思考較少人討論的遊戲產業之洗錢風險及相關持續性稽核機制。

參、研究方法

本研究採用之方法為訪談遊戲業相關業者，了解其公司主要活動運作流程，再以電腦輔助稽核軟體設計持續性稽核的作業，以協助遊戲業即時發現並處理問題。

一、深度訪談

本研究根據文獻探討分析所得之資料，加以整理，擬訂訪談題目，透過深度訪談法來取得對遊戲業者作業流程的了解，以瞭解遊戲業相關人員對遊戲業主要期望為何，並分析遊戲業主要活動之運作方式，透過了解其作業活動，尋求可供設計出持續性稽核之控制點及相關活動。

二、持續性稽核作業的設計

隨著資訊科技的進步，稽核人員已開始轉向使用 E 化稽核工具，由原先傳統的人工抽樣稽核，轉變成利用科技輔助的自動化稽

核系統來處理日常的稽核作業，在 E 化下的內部控制，可減少人為疏失所造成的錯誤，提高工作自動化程度，省下更多的時間與資源。

本研究運用電腦輔助稽核軟體協助取得大量資訊並進行資料分析來設計持續性稽核作業。電腦輔助稽核工具選擇 ACL（ Audit Command Language，以下簡稱 ACL）軟體，利用虛擬資料庫檔案進行測試，依據電腦稽核系統的處理邏輯，進行平行模擬試算或是分析，將試算分析的結果進行比對，針對差異的部分再進行了解與分析。

現行常見的電腦輔助稽核軟體包括有 ACL、IDEA、EXCEL 等，然而以被使用及受歡迎程度而言，ACL 是其中的佼佼者。雖然 EXCEL 是最易於接觸到的一種，但在目前巨量資料的情況下，會有資料筆數限制的問題，而相對來說，ACL 具有可以處理海量資料、可以讀取多種資料來源檔案格式、可以確保來源資料的完整性與安全性等功能，這是本研究選擇此工具的原因。

透過文獻回顧、深度訪談以及本研究小組實際觀察後，本研究擬將持續性稽核作業的設計聚焦於點數銷售及安全性作業，並試圖從中設計出持續性稽核程式，以作為遊戲公司洗錢風險防治之機制。

肆、實證結果與分析

一、深度訪談

經由訪談以及實際觀察後的結果，發現有以下流程可能在作業過程中產生疏失：玩家購買點數較常使用之通路為超商與第三方支付平台 (例如：橘子支)，然而在退款機制中，超商只需確認發票且未儲值即可，另一第三方支付平台只需確認未儲值且退款帳戶可隨時更動，這交易過程中，有可能成為洗錢風險之一。

故本研究將針對此部分進行遊戲業者虛擬資料模擬的持續性稽核作業程式。

二、點數銷售及交易安全性稽核作業

根據第貳部分文獻探討所述網路的發達帶來不少便利，卻也造就有心人士利用不法手段獲取利益，加上近年來遊戲業的蓬勃發展，高單價的點數交易及買賣點數後可退款之服務，可能是造就洗錢的原因之一，故本研究運用以下兩個測試，協助遊戲公司能提前預防以免淪為洗錢管道。

1. 超商點數銷售測試：以超商點數銷售資料檔抓取高單價交易資料。
2. 交易安全性測試：連結橘子支會員檔抓取退款帳號與上次不同之會員帳號。

（一）超商點數銷售測試

因超商代收上限為個人單筆兩萬元，本研究折衷後以單筆一萬元列為高風險基礎，透過測試得到高風險超商銷售分店。茲將點數銷售稽核之規劃列於表 1，持續性稽核程式圖則列示於附錄中，以供參考。

表 1　超商點數銷售專案規劃

查核項目	超商點數銷售	存放檔名	超商銷售點數
查核目標	找出高風險銷售的超商分店		
查核說明	查核點數交易總額異常多的超商，特別予以關注。		
查核程式	(1) 連結點數序號，驗證出點數銷售時間等於點數產生時間 (2) 萃取點數交易金額大於等於一萬，找出高風險銷售分店		
資料檔案	Excel		
所需資料表	D 2- 1 玩家儲值資料檔、D 2- 2 公司銷售資料檔、D 2- 3 超商點數銷售資料檔		
所需欄位	點數序號、點數產生時間、點數交易金額、點數銷售時間 … 等		

（二）交易安全性測試

本研究對

1. 有變更退款帳號之會員；2. 月取消交易頻繁的會員進行稽核測試，取消交易時間以六月為範例，退款次數基準值為；3. 透過測試得到退款次數異常之會員。茲將安全性稽核之規劃列表於表 2，持續性稽核程式礙於篇幅，不予列示。

表 2　交易安全性專案規劃

查核項目	超商點數銷售	存放檔名	超商銷售點數
查核目標	找出交易退款帳號異常與退款次數異常的會員資料		
查核說明	若頻繁變更退款帳號或退款次數大於等於 3，將持續追蹤會員，預防洗錢的可能性。		
查核程式	(1) 取消交易時間不等於空值，找出點數交易異常資料 (2) 連結橘子支會員帳號，找出交易異常會員的退款帳號 (3) 連結會員等級，萃取每月退款次數大於等於基準值 (4) 最終找出交易異常會員裡的退款次數		
資料檔案	Excel		
所需資料表	D 2- 4 點數交易檔、D 2- 5 橘子支會員檔		
所需欄位	取消交易時間、上次退款帳號、本次退款帳號、橘子支會員帳號、會員等級 … 等		

伍、結論與建議

本段將針對研究發現與稽核測試之結果進一步說明，並根據研究結果，對遊戲業者、政府機關及後續研究者提出建議。

一、研究結論

藉由深度訪談及本研究小組實際觀察，進行超商點數銷售測試、交易安全性測試，本研究利用電腦輔助稽核軟體進行測試取得模擬資料之結果，並從文獻與訪談回顧後可知，消費者可透過超商及第三方支付平台購買點數，根據本研究小組實際測試後發現，超商及第三方支付平台的退款機制較於簡易，有心人士可能藉此漏洞進行違法的動作 (例如：洗錢)，因此可以透過稽核程式，定時偵測交易較於異常的超商分店及第三方支付平台之帳號，後續將稽核程式放置於持續性稽核的平台中，並利用資料倉儲或是連結開放性資料庫 (Open Database Connectivity，ODBC) 的方式，即可達到自動化持續性稽核之效果。

二、研究建議

根據本研究之發現，研究小組提出以下之建議，以做為遊戲業者、政府機關及後續研究者之參考。

（一）對遊戲業者之建議

1. 超商點數銷售通路之改善

本研究小組在進行研究時發現，目前超商通路的點數是無實名制販售，在購買金額也沒有上限額度，且退款僅需確認發票跟序號尚未儲值即可，在這樣的情形下，可能造成有心人士拿來作為洗錢的管道，因此本研究小組建議可以規定超商多媒體機台買票前要先輸入買家身分證字號，實名登記，或是皆採電子支付方式（悠遊卡、第三方支付等），因電子支付具有實名制效果，有利於事後追蹤購買者。

2. 第三方帳號之規定

本研究小組在研究進行時發現，於退款時變更退款帳號，橘子支並沒有更進一步確認使用人之相關個資，且並無明確規定退款上限，都將可能導致有心人士利用騙取金錢。另外，本研究對橘子支退款帳戶是否為本人親自持有之帳戶，無法做進一步確認，故本研究僅針對頻繁變換退款帳戶支使用者進行稽核。

（二）對政府機關之建議

本研究小組在實際觀察與研究後發現，點數販售通路尚有屬於未記名的交易方式，為預防有心人士透過遊戲虛擬貨幣來進行洗錢行為，故本研究小組建議政府應透過法令將遊戲虛擬貨幣的交易轉為實名登記制或者禁止透過未記名交易通路，減少洗錢的行為發生，也便於日後發生疑義。

（三）對後續研究者之建議

本研究限於時間和資料敏感性方面等客觀因素，且因遊戲產業結合金融科技牽連甚廣，細節上無法一一探討，因此，本研究僅探討電子支付、第三方支付的相關事項。在安全性稽核作業中本研究小組係以第三方支付橘子支為例，針對橘子支綁定帳號產生帳號異動者，並無法判斷出是否為本人使用中之帳號，且沒有明確規定退款上限，所以本研究小組建議後續研究者可以進一步探討其餘第三方支付之使用方法及高金額退款以便設計相關之稽核程式。

參考文獻

1. 吳淑娟，2015，行動支付之風險因子探討 – 以第三方支付為例，電腦稽核半年刊，32，105- 108
2. 法務部調查局，2016，洗錢防治工作年報，p 53- 55
3. 柳哲豪，2017，從遊戲到電子支付—歐買尬的轉型策略，國立臺灣科技大學資訊管理系碩士在職專班碩士論文
4. 張中一，2016，金融科技發展簡介與芻議，電腦與通訊，167 特刊，4- 12
5. 張孟妍，2017，金融機構洗錢防制之探討，中國文化大學法學院法律系在職專班碩士論文
6. 許義寶，2012，洗錢犯罪，於汪毓瑋主編，跨國（境）組織犯罪理論與執法實踐之研究（分論），台灣：元照出版，1- 32

7. 猴集仁，2012，金融機構帳戶管理對洗錢防制之關聯性研究，義守大學管理學院管理碩士在職專班碩士論文

8. 蘇裕惠，2006，內部稽核強化公司治理，內部稽核季刊，53，4- 8

9. Newzoo：2017 年全球遊戲市場報告，https://www.useit.com.cn/thread- 15855- 1- 1.html

10. 人民日報，2017 年 07 月 07 日，電子支付面臨惡意詐騙等新挑戰 無現金社會還有多遠？ http://it.people.com.cn/BIG 5/n 1/ 2017/ 0707/c 1009- 29389133.html

11. 工商時報，2017 年 12 月 25 日，台灣瘋電競 外商、新創搶進，http://www.chinatimes.com/newspapers/ 20171225000326- 260204

12. 中央社新聞，2017 年 12 月 26 日，賣網遊虛寶及點數未報稅 補帶罰近 8 百 萬，http://www.cna.com.tw/news/afe/ 201712260220- 1.aspx

13. 中國證券報中證網，2016 年 12 月 07 日，加快購建 P 2P 洗錢風險防控體系 http://www.cs.com.cn/sylm/zjyl_ 1/ 201612/t 20161207_ 5112727.html，

14. 內政部警政署，2017 年 03 月 08 日，中華民國內政部警政署警政治安全球資訊網，https://www.npa.gov.tw/NPAGip/wSite/ct?xItem= 83129&ctNode= 12594&mp= 1

15. 蘋果日報，2017 年 07 月 01 日，遊戲詐騙旺季來了 宅男上當率高居榜首，https://tw.appledaily.com/new/realtime/ 20170701/ 1152229/

16. 蘋果日報，2017 年 11 月 10 日，國際奧會認可電競是運動 2024 巴黎奧運或會登場，https://tw.appledaily.com/new/realtime/ 20171110/ 1238506/

附錄

圖 2 超商點數銷售測試稽核程式

```
IMPORT EXCEL TO D2_1 玩家儲值資料檔 "C:\Users\user\Desktop\3\D2-1 玩家儲值資料檔.fil" FROM "玩家儲值資料檔.xlsx" TABLE "玩家儲值資料檔$" KEEPTITLE FIELD "遊戲公司帳號" C WID 13 AS "" FIELD "遊戲帳號" C WID 13 AS "" FIELD "點數序號" C WID 10 AS "" FIELD "點數交易金額" N WID 4 DEC 0 AS "" FIELD "點數儲值時間" D WID 19 PIC "YYYY-MM-DD hh:mm:ss" AS ""
OPEN D2_1 玩家儲值資料檔
IMPORT EXCEL TO D2_2 公司銷售資料檔 "C:\Users\user\Desktop\3\D2-2 公司銷售資料檔.fil" FROM "公司銷售資料檔.xlsx" TABLE "公司銷售資料檔$" KEEPTITLE FIELD "交易超商分店" C WID 3 AS "" FIELD "點數產生時間" D WID 19 PIC "YYYY-MM-DD hh:mm:ss" AS "" FIELD "點數序號" C WID 10 AS "" FIELD "點數交易金額" N WID 4 DEC 0 AS ""
OPEN D2_2 公司銷售資料檔
OPEN D2_1 玩家儲值資料檔
OPEN D2_2 公司銷售資料檔 SECONDARY
JOIN PKEY 點數序號 FIELDS 遊戲公司帳號 遊戲帳號 點數交易金額 點數儲值時間 點數序號 SKEY 點數序號 WITH 點數產生時間 交易超商分店 IF 點數儲值時間 <'20170101' TO "T2-1-1 未儲值點數資料" OPEN PRESORT SECSORT ISOLOCALE root
OPEN "T2_1_1 未儲值點數資料"
IMPORT EXCEL TO D2_3 超商點數銷售資料檔 "C:\Users\user\Desktop\3\D2-3 超商點數銷售資料檔.fil" FROM "超商點數銷售資料檔.xlsx" TABLE "超商點數銷售資料檔$" KEEPTITLE FIELD "點數序號" C WID 10 AS "" FIELD "超商分店代號" C WID 4 AS "" FIELD "點數交易金額" N WID 4 DEC 0 AS "" FIELD "點數銷售時間" D WID 19 PIC "YYYY-MM-DD hh:mm:ss" AS "" FIELD "點數退貨時間" D WID 16 PIC "YYYY/MM/DD HH:MM:SS" AS ""
OPEN D2_3 超商點數銷售資料檔
OPEN T2_1_1 未儲值點數資料
OPEN D2_3 超商點數銷售資料檔
INDEX ON 點數序號 TO "D2_3 超商點數銷售資料檔_on_點數序號" ISOLOCALE root
OPEN T2_1_1 未儲值點數資料
DEFINE RELATION 點數序號 WITH D2_3 超商點數銷售資料檔 INDEX D2_3 超商點數銷售資料檔_on_點數序號
SUMMARIZE ON 交易超商分店 點數產生時間 SUBTOTAL 點數交易金額 OTHER 遊戲公司帳號 遊戲帳號 點數序號 點數交易金額 點數產生時間 D2_3 超商點數銷售資料檔.點數銷售時間 D2_3 超商點數銷售資料檔.超商分店代號 交易超商分店 TO "T2-1-2 按時間加總金額.FIL" OPEN PRESORT ISOLOCALE root
OPEN "T2_1_2 按時間加總金額"
VERIFY FIELDS COUNT 交易超商分店 超商分店代號 遊戲公司帳號 遊戲帳號 點數交易金額 點數序號 點數產生時間 點數銷售時間 ERRORLIMIT 10 IF 點數銷售時間 = 點數產生時間 TO SCREEN
EXTRACT RECORD IF 點數交易金額 >= 10000 TO "A2-1-1 高風險超商銷售分店" OPEN
OPEN "A2_1_1 高風險超商銷售分店"
```

財報不實民事損害賠償額計算之研究

The Study on the Calculation of Civil Liability for Financial Statement Attestation

許淑媛 Cadalina Hsu
台灣大學法學士/碩士，中正法博士班，大洋法律事務所執行長
B.A./M.A at NTU, P.H.D. Student at CCU,
C.E.O. at Da-Young attorney-at-law firm.

摘　要

2006 年增訂之證交法第 20 條之 1，目的在明確、強化財報不實之民事損害賠償責任。然其部分內容在學理上備受質疑，例如將「有價證券持有人」列為損害賠償請求主體之妥當性。部分內容在實務運作上遭遇困難，例如不實財報與損害之間因果關係之舉證、過失比例責任之認定及損害賠償額之計算等。本文嘗試參酌外國學理及實務見解就此等問題予以釐清。

關鍵詞：持有人、交易因果關係、市場詐欺理論、損失因果關係、過失比例責任。

Abstract

In 2006, the Securities and Exchange Act added the status 20 of 1 to clarify and strengthen the civil liability for financial statement attestation. However, there is a highly contentious question among practitioners and scholars, such as the rationality of adding "the securities holder" as the subject of the financial statement fraud. Besides, there are lots of difficulties and gaps between rule and the reality, for example, the burden of proof

in the causality between financial statements and civil damages, the definition of the proportion of Degree of Fault and the calculation of the amount of civil compensation, and so on. The study analyzes the judicial verdicts and theoretical opinions from the foreign countries, and try to let the issues to be clarified.

Keywords：Securities holder, Transaction causation, Fraud on the market theory, Loss causation, Proportionate liability.

壹、前言

按我國現行證券交易法第 20 條第二項，明定：「發行人依本法規定申報或公告之財務報告及財務業務文件，其內容不得有虛偽或隱匿之情事。」；而於 2006 年修正新增之證券交易法第 20 條之一復規定，若上開條文中所稱之財務及業務文件，及依證券交易法 36 條第一項公告及申報之年度財務報告、季報、月報等財務報告，其主要內容有虛偽或隱匿之情事時，發行人及其負責人、職員、簽證會計師等賠償義務人，對發行人所發行有價證券之善意取得人、出賣人或持有人因該情事所受之損害，應負賠償責任，此即學理上所稱之財報不實損害賠償責任。

而上開條文中，雖揭示該賠償責任為民事「侵權行為損害賠償」責任之定性，然而，對於該受害投資人損害金額之計算方式，則未見著墨。遍查證券交易法，針對如財報不實、公開說明書不實、操縱股價、內線交易等證券詐欺行為之類似規定，僅於 157 條之一第三項中有明定內線交易受害投資人之損害擬制計算方式[1]，餘則未見明文，故學界與實務家對此多有主張及爭論，本文試透過相關文獻及實務判解之整理分析，期對財報不實情事中，受害投資人所受損害額之計算，有深入之了解。

貳、損害賠償額估算方式之介紹

受害投資人因財報不實所致之損害，主要係由於股價下跌所生。而股價下跌之因素，固有基於揭露不實資訊所致，然而亦有可能因其他介入市場之因素所肇致。因此計算其所受損失時，是否需排除其他市場因素之影響，則成肯否二說，如認無須排除市場因素之計算法，學理上則稱為「毛損益法」[2]；而如認須排除市場因素之計算方法，學理上以「淨損差額法」稱之，以下分述之：

一、毛損益法

毛損益法，其旨以回復受害投資人至交易前之經濟應有狀態為原則[3]，其以受害

1. 證券交易法 157 條之一第三項規定：「違反第一項或前項規定者，對於當日善意從事相反買賣之人買入或賣出該證券之價格，與消息公開後十個營業日收盤平均價格之差額，負損害賠償責任；其情節重大者，法院得依善意從事相反買賣之人之請求，將賠償額提高至三倍；其情節輕微者，法院得減輕賠償金額。」
2. 葉新民，論資本市場上因不實資訊而致投資人損害的賠償方法－以德國法為中心，中原財經法學，23 期，頁 48。
3. 莊永丞，證券交易法第二十條證券詐欺損害估算方法之省思，臺大法學論叢，34 卷 2 期，頁 13。

投資人於資訊公布前買入股票之價格，減去消息揭露後，真實出賣股票之價格，得出其所受損失額[4]。其論理依據為，如無該等虛偽不實記載，被害投資人自始不可能購入該證券[5]，換言之，如受害投資人知悉該財務報告內容為不實，根本不會做成自交易市場買受該股票之決定，故賠償義務人自應就受害投資人因作成投資買受股票之全額損失負責[6]。

二、淨損差額法

淨損差額法，其旨為填補受害投資人所受之損失，因此其所能請求之損害，自僅限於與賠償義務人之不實財報等詐欺行為具因果關係者。如非義務人之詐欺行為所致，而係其他影響市場因素所致之下跌，全令賠償義務人負擔，即有失適當。故其計算方式，係以買進時之市價，減去該股票擬制之「真實價值」所得之差額[7]。

然而，此說所面臨之最大困難，即為擬制真實價格之認定。論者有謂，固然可以消息揭露、更正後，當日股市交易的收盤價以定，因消息一旦揭露，股價即不受消息影響，回復其原狀，但現實而言，消息揭露後市場常產生過度之恐慌性賣壓，反致股價無法反映真實價格[8]。因此，實務上常需借助財務經濟學專業判斷，於美國司法實務上，Green v. occidental petroleum corp. 一案中，Sneed 法官將「不實資訊發布之日」與「該資訊被揭穿或更正之日」間，劃出兩條折線，一為受不實資訊影響下，股票價格實際波動之「價格線」，一則為擬制無不實資訊影響下，股票應有價值之真實「價值線」，而受害投資人所受之損失即為各交易日兩線之差距[9]。

彼邦實務中，財務經濟學專家多以市場模型，運用「指數比較法」及「事件研究法」以計算真實價格 (價值線),「指數比較法」中，真實價格為一持平之固定數字，價值線為一長水平線，而該真實價格之發現，則以類似我國證券交易法於 157 條之一中擬制十營業日收盤均價之作法，以該不實資訊更正後之一定期間內，推算受到該消息影響後之單一真實股價，即該期間之交易均價；而「事件研究法」中，真實價值與市場股價間，恆維持一定程度之係數關係，價值線係隨價格線以一定之關係波動，故採事件研究法時，每日均會有一不同數值之真實價格，受害投資人之買進時點，直接影響其損失額之認定[10]。

叁、學者見解

因我國實務中，如美國實務般，趨向採取「淨損差額法」作為計算損害金額之態勢已漸明顯，擬制之真實價格即成為勢必積極

4. 同註 4。
5. 劉連煜，新證券交易法實例研習，2014 年 12 版，頁 375，元照。
6. 劉連煜，財報不實案中有關證券持有人的舉證、過失比例責任及會計師事務所之連帶責任－台灣高等法院 101 年金上字第 7 號民事判決評釋，法令月刊，64 卷 12 期，頁 17；該號判決文參照。
7. 莊永丞，前揭文，頁 7。
8. 同註 4。
9. 劉連煜，財報不實損害賠償之真實價格如何認定及投資人是否與有過失問題－最高法院 102 年台上字第 1294 號等民事判決研究，月旦法學雜誌，232 期，頁 240。
10. 劉連煜，財報不實之損害賠償責任：法制史上蜥蜴的復活？－證券交易法新增訂第二十條之一的評論，月旦民商法雜誌，11 期，頁 61。

面對與解決之問題。然而，論者主張，如若彼邦採用「事件研究法」進行分析，勢必極度倚賴鑑識會計技術，財務經濟學相關之專家證人之延攬亦必墊高訴訟之成本負擔，如以訴訟經濟之觀點，於我國未必為適宜之損害額計算法。故其主張，可將各不實財報公布後之一定期間，認定為受該次不實財報影響之期間，進而計算該期間內之一個擬制真實價格，似無逐日個別計算每一投資人之擬制真實價格之必要，而此一定期間，於資訊揭露後之九十日或十營業日之平均收盤價均為可行的選項[11]。此種主張，似與我國近期實務中最高法院所採取近似於「指數比較法」之擬制真實價格計算方式較為接近。

然而，如我國實務中採取「指數比較法」計算真實價格下，該一定期間究以幾日為佳？此與市場之「適當反應期間」及息息相關，換言之，市場究需多久期間方能充分反映該事件之影響？我國有參考美國立法例，以彼邦 1995 年「私人證券訴訟改革法」(Private securities litigation reform act) 第 21D(e) 條關於損害賠償額計算上限之規定以 90 日計算者，然該上限規定，論者亦有批評，謂該期間過於漫長，致過多市場因素介入，有影響股價漲跌之可能，另如該股票於期間內因其他市場因素而大漲，因而使該均價與受害投資人之買價差距拉近，該利益均歸於賠償義務人獨享，對受害投資人亦不甚公平[12]。亦有參考證券交易法中關於內線交易之規定而以 10 日計者[13]。此目前仍尚無定論，亦為我國實務上最高法院常持以撤銷發回原審判決之理由[14]。

惟亦有論者參酌德國學說觀點，認為應分別原告 (即受害投資人) 回復原狀或金錢賠償二種情形，而異其處理方式。今如受害投資人主張回復原狀，該「原狀」係指如被告 (即賠償義務人) 未隱匿或公布不實資訊時，受害投資人本來所有之財產狀態，即為無購入股票之狀態，換言之，即主張「被騙而買」時，如受害投資人確能舉證受到詐欺而買入股票，而其購入股票係因受到詐欺，陷入錯誤決策之結果，即代表已證明「交易因果關係」之存在，此情形下，其無須舉證其所受損害額，而被告須返還全數購股價金，但「交易因果關係」之標準仍容有爭議；但如受害投資人主張金錢賠償，其所主張者，其實為該不實資訊致市場價格遭到扭曲，致其以被高估之價格買入該股票，換言之，即為主張「買貴了」，此情形下，其即無須證明「交易因果關係」，僅須證明「損失因果關係」，即其買賣股票之損害，係因證券詐欺或不實資訊所致即可。然此時即須以「淨損差額法」計算，以免將市場因素計入損害之不公平現象，而僅須賠償受害投資人真實價格與其買價之差額。換言之，如受害投資人有能力舉證「交易因果關係」，即採「毛損益法」，認其得以請求回復原狀之完整利益；而如「交易因果關係」之舉證有困難，則其僅採「淨損差額法」，請求價值利益[15]。

11. 劉連煜，同註 10 文，頁 243。
12. 何曜琛、陳盈如，資訊不實民事損害賠償之過失相抵－最高院 102 台上 1305 判決，台灣法學雜誌，251 期，頁 184。
13. 林國全，財報不實之民事責任，月旦民商法雜誌，48 期，頁 29。
14. 如最高法院 102 年台上字第 1305 號民事判決。

以上觀點與日本學界所持之主張似有相類，彼邦學界將財報不實致投資人所受之損害，分為侵害「投資人購入該證券之自己決定權」或侵害「投資人購入該證券高於真實價格之財產權」二面向以觀，如為侵害「投資人購入該證券之自己決定權」者，因其侵害者為投資人之自我決定權，其損賠責任在於恢復其未購入該證券之財產狀態；而如侵害「投資人購入該證券高於真實價格之財產權」者，既為財產權侵害，其責任則僅在於賠償投資人買賣證券價格與真實價格之間之價差，因此，前者自應以「毛損益法」計算回復原狀之損害賠償，彼邦學界以「取得自體損害說」稱之；後者則以「淨損差額法」賠償其價格差額，彼邦學界則稱之為「高額取得損害說」[16]。然而，後彼邦對於此種投資人於流通市場買賣證券，因財報不實所受之損害，增訂「金融商品取引法」第 21 條之二規定，對其損害額採取推定方式為之，以資訊更正前一個月該證券市場價額之均價，扣除資訊更正後一個月該證券市場價額均價，即為損害額。然此僅係損害額計算方式之一，論者謂，如投資人得以其他計算方式證明其實際受害金額，仍得依其計算求償，抑或投資人亦得主張其受侵害者為自我決定權，要求回復原狀之損害賠償[17]。

但同時亦有論者提出不同主張，其謂損失因果關係之認定，牽涉司法解釋及法律政策之選擇，如採「預見可能性說」，限縮為行為人僅就其為侵權行為時所能預見之損害負責者，則應偏向「淨損差額法」之適用；而如採取「直接因果關係說」，擴張行為人需負責之範圍致其侵權行為所致之全部損失，不論行為人於行為時有無預見之可能者，則較偏向「毛損益法」之適用效果，故法院實務上得以被告 (即賠償義務人) 之不法行為係出於故意或過失，而分別採用不同損失額計算方法，故意行為則以「毛損益法」計算受害投資人所受之損失額；而過失行為則以「淨損差額法」計算受害投資人之損失，而異其處理[18]，以求其公平。而賠償義務人所為之不法行為如係故意行為時，以「毛損益法」計算受害投資人所受之損失額，是否有涉及「懲罰性賠償」的問題，其則採否定見解，認此僅係損失因果關係認定之問題而已，而非處以一定之數額或倍數之賠償金處罰，故與「懲罰性賠償」無涉[19]。然而，如採此見，損害賠償數額之計算方式，是否宜因行為人歸責程度不同而有所歧異？

肆、我國實務中對損害額之計算

諸如財報不實等證券詐欺案件，迭見於我國實務中，而我國法院於個案審理時，看法也各見歧異。本文整理數則於學界討論密度較高之實務判決，期能一窺我國法院歷來見解之趨勢與流變。

一、順大裕案 (臺灣臺中地方法院 90 年重訴字第 706 號民事判決)

本件中法院肯認原告等採「毛損益

15. 葉新民，前揭文，頁 159 以下。
16. 林麗香，財報不實損賠責任之計算－最高院 104 台上 225 判決，台灣法學雜誌，296 期，頁 182。
17. 林麗香，前揭文，頁 183。
18. 同註 13。
19. 同註 13。

法」請求被告連帶損害賠償之金額，其論述謂，若被告(賠償義務人)等人將公司財務、營業狀況予以確實揭露，無故意詐欺行為，則原告(即受害投資人)等不可能認購或買進順大裕公司股票，故受害投資人所主張之「如有於起訴前賣出之情形時，依買進或認股之金額與賣出之金額計算價差，…；至於未賣出而仍持股部分，則以認股價格或買進價格與八十九年二月平均收盤價值（七元）之差額計算」，「參以被告順大裕公司業經本院裁定終止重整，股票亦已自集中交易市場下市，並參照前述我國實務先例及外國相關規定之法理，本院認原告等主張之損害賠償金額之計算方式，堪以採取。」

嗣後本件上訴至高等法院時，臺灣高等法院臺中分院於93年金上字第2號民事判決中亦指出：「若無彼等故意詐欺行為，而將公司財務、營業狀況予以確實揭露，則乙〇等五百八十一人焉有認購或買進順大裕公司股票之理？爾後自不可能因違約交割之事件爆發而蒙受加重損害，是以在此故意詐欺之情形下，若將往後的市場風險均令乙〇等五百八十一人之一般投資大眾負擔，顯失公平。」

二、大中鋼鐵案（臺灣臺中地方法院91年訴字第243號民事判決）

本件中，法院指出：「股價變動之因素非單一，是尚難僅以原告(即受害投資人)買進賣出之差價，即認係原告因被告行為所受之損害。」然而，其對損害額之計算，則表示「欲精確排除各種非人為因素而計算原告所受之損害，顯有重大困難。」，故其審酌受害投資人於買進大中公司股票，至賣出股票期間，鋼鐵類股中扣除特別股之平均跌幅與大中鋼鐵個股跌幅之差額部分，「可認係大中鋼鐵超逾一般鋼鐵類股平均跌幅之部分，爰以之做為計算原告得請求被告賠償之依據。」，嗣後經臺灣高等法院臺中分院以92年上易字第471號民事判決駁回上訴。

無獨有偶，最高法院於大中鋼鐵公司另案，100年台上字第640號民事判決中，亦指出：「上訴人雖確實受有損害，惟其所為請求賠償金額，應以回復至應有狀態為據」，故原審法院「進而論斷應以不實訊息被揭露翌日之股價，與上訴人買入股價差額百分比，扣除與不實訊息公告無涉之市場同類股大盤跌幅百分比，再乘以買入價格，作為計算方式，…殊難認有何違背法令之處。」亦採上述臺中地院相同之見解，估算市場因素造成之損害時，採取所謂「類股指數比較法」，將同類股之損失部分加以扣除，被告僅就超跌部分負擔賠償責任[20]。

三、立大農畜案（臺灣高等法院高雄分院94年金上字第1號民事判決）

本案中法院係採用「毛損益法」計算受害投資人之損失，其指出：「…在計算投資人因資訊、財報不實所致損害時，自得假設投資人若非因資訊未真實揭露，即不至於買入該股票，則其損害應為該買入股票之價格，扣除其於資訊揭露後出售股票之價格，或未出售股票者，扣除起訴時股票價格，始合乎公平。…」

而如受害投資人因該股票已暫停交

20. 劉連煜，同註10文，頁241。

易、甚至下市，致至判決時尚未出售持股時，其則以「參以主管機關證期會 93 年 1 月 28 日台財證三字第 0920156565 號函表示：如所買賣之上市、上櫃股票因特定事件之影響，導致公告暫停交易，若該事件揭露後至暫停交易日之期間，已足供市場適當反應該事件對股價之影響，且暫停交易後並無發生重大影響公司股東權益之情事，可參考證券發行人財務報告編製準則第八條第三項第一款第二目規定，按暫停交易日前一個月之平均收盤價格作為暫停交易後之參考價格。」以暫停交易日前一個月之平均收盤價格，計算受害投資人未出售股票部分之股價損失。

然而，本件後經上訴至最高法院時，竟以 97 年台上字第 1118 號民事判決發回更審，該案後臺灣高等法院高雄分院 97 年金上更 (一) 字第 2 號更審判決中，該院則改採「淨損差額法」計算受害投資人之損失額，其指出「被上訴人因誤信上訴人不實之財務報告而高價購買股票，該公平合理價格應以不實情事揭露後 90 個營業日收盤平均價，擬制為該有價證券未受不實財務資訊影響之所謂『真實價格』，故計算投資人損害，應以該真實價格與被上訴人購買價格之差價，以填補被上訴人之損害，…」

四、日昇案 (臺灣高等法院臺中分院 99 年建上字第 18 號民事判決

本案中高等法院係採取「毛損益法」計算受害投資人之損害額，其指出：「按投資人受不實財務報表詐欺買入股票並繼續持有，應以其買入時之股價乘上持有之股份總數，扣除請求賠償時公司每股淨值乘上持有之股份總數，所得金額作為賠償之計算。」

然而最高法院以 102 年台上字第 1305 號民事判決，其以：「被上訴人獲悉上訴人不法行為至提起本件訴訟亦長達數月，則市場適當反應該項重要訊息所需之期間為何？倘被上訴人於適當反應期間內未出脫持股導致擴大其損害是否與有過失，核與應否減免上訴人之賠償責任攸關。原審未遑詳查究明，遽以前揭情詞為不利於上訴人之論斷，自有可議。」將原判廢棄發回。

五、宏億案 (臺灣高等法院 101 年金上字第 7 號民事判決)

本件承審法院對「毛損益法」及「淨損差額法」二種常見之計算方式有清晰之說理：「依毛損益法而言，不論差額係不實財報引起或其他市場因素所造成，賠償義務人均應承受股價下跌之結果而負責賠償；蓋投資人若知悉財務報告內容為不實者，根本不會作成自發行市場或交易市場買受股票之決定，故認為賠償義務人應賠償投資人因作成投資而買受股票之全部損失。」而，「倘依淨損差額法，賠償義務人僅賠償因不實財報因素造成之股價損失，即股票『真實價值』與『買價或賣價』間之差額，至於市場因素造成之股價下跌不在賠償範圍。」

然而，其不採以「淨損差額法」計算所受損失，並類推適用證券交易法第 157 條之一中內線交易損害賠償，以消息公開後十營業日收盤均價之計算「真實價格」之主張，而係明採「毛損益法」計算。其指出：「雖主張應依證交法規定，以不實財報消息揭露後 10 個營業日收盤平均價格，作為「股票真實價格」…；惟證交法第 157 條

之 1 規定係就內線交易損害賠償之計算方式，核與投資人因財務報告不實所受之損害型態迥異，尚難以不實財報消息揭露後 10 個營業日收盤平均價格，作為『股票真實價格』，而依淨損差額法計算投資人因不實財報所受之損失。」

其明確採取「毛損益法」，指出「依一般客觀情形判斷，正常理性之投資人若知悉宏億公司真實之財務及業務狀況且有隱匿備抵存貨跌價損失情形者，應無任何意願作成買受宏億公司股票之舉措，是本院認為第一類授權人因系爭財報不實所受股價下跌之損失應採取前開毛損益法計算損害，始符公允。」

然而，本件上訴至最高法院時，最高法院於以 104 年臺上字第 225 號民事判決指出：「損害賠償之目的在填補所生之損害，其應回復者，並非「原來狀態」，而係「應有狀態」，自應將非可歸責於債務人之變動狀態加以考慮，認僅應有狀態之損失始與不實財報間有因果關係。」，因此「第一類授權人請求原判決附表甲所受股價下跌之損失，是否可認與系爭財報不實間有因果關係，亦非無疑。原審未遑詳查究明，復未說明就此防禦方法之取捨意見，遽引詐欺市場理論，依毛損益法計算損害金額而為渠等不利之判斷，自屬可議。」將此部分判決廢棄，撤銷發回。

六、訊碟案（最高法院 102 年臺上字第 1294 號民事判決）

本案中，最高法院則明文肯認原二審法院以「淨損差額法」作為損失額之計算標準，其指出：「查上訴人財報資訊不實期間，其股票市價因受不實財報資訊之影響而呈現虛漲狀態，附表所示投資人於上開期間內，於公開市場買進上訴人股票，即受有『市價』與『真實價格』間價差之損害，投資人所受損害，應以『淨損差額法』即投資人購買價格減去股票真實價格之差額計算之，始為合理。」

而真實價格之計算，其指出：「所謂『真實價格』，係指若無詐欺因素的影響，股票所應有的價值」，然而，其並未採用「事件研究法」推算，而以「指數比較法」，「參較證券交易法第一百五十七條之一關於內線交易以不實消息公開揭露後十個營業日收盤平均價格為計算差價基準、美國法例以不實消息更正日起九十日平均價格擬制為『真實價格』、及第一審所採之毛損益法計算之結果」，認定以「…虧損重大訊息公開揭露後十個營業日收盤平均價格三．三七八元，擬制作為計算投資人損害之真實價格，較為妥當公平。」

七、小結

由此觀之，我國實務於前期似有偏好採取「毛損益法」作為損害額計算方式之走向，然最高法院近期自「立大農畜案」以降，似有逐漸向「淨損差額法」靠攏之趨勢，102 年臺上字第 1294 號判決中更明示肯認「淨損差額法」，然而，於目前實務中卻未見如前述美國法院般，引入財務經濟學專業，以「事件研究法」等科學方法計算擬制之「真實價格」，而似較接近「指數比較法」由消息揭露後，選定一定期間內之均價，以類似證券交易法第 157 條之一中內線交易受害投資人之損害擬制方式，以該均價作為「真實價格」之基準線 (價值線)。

伍、結語

綜上，如美國「私人證券訴訟改革法」或日本「金融商品取引法」等立法例，對於不實財報致受害投資人損失之賠償額計算方式，有以「上限」或以「推定」等方式，此般規範雖非強制性、唯一之計算標準，然其不僅可提供法院實務於個案認定時可資參酌，亦可折服涉訟兩造，收定紛止爭之效。然我國證券交易法中，因乏此種於不實財報情形下，對受害投資人損失額計算之實定法規範可循，故實務上常因兩造迭有爭執指摘，致案件一再更審，久延不決。本文主張，就立法論上而言，似可參採如前述美、日等國之立法例，研擬如證券交易法第 157 條之一內線交易之損害賠償責任般，訂立於財報不實之情形，相應之損害計算標準。

現行法制下，究應用何種計算標準，以能顧及受害投資人損失之完整填補及免對賠償義務人加予過重且無法預期之負擔，本文看法則與現行實務較為接近，認同以「淨損差額法」排除因其他市場因素所致之損害，較能兼顧事理之衡平。然正如上述論者所陳，如採「事件研究法」進行真實價格之分析，勢必無可避免地墊高訴訟成本，鑑於我國鑑識會計人才仍未充實之現實環境，似無徒增兩造當事人及承審法院之勞費，而遽然引進「事件研究法」之必要，故論者以為[21]，「指數比較法」似為相對較佳之可行途徑，本文從之。至於擬制受該事件影響之期間，目前實務看法兩歧，有主張類推適用內線交易損害賠償責任之 10 日基準者，亦有參考美國立法例以 90 日為準者，俱有其論理依據，然市場充分反映一財報不實事件之影響之期間，究應如何認定，方為符合我國國情與市場特性，則仍有待國內先進學說發展與實務判例之累積。

參考文獻

1. 何曜琛、陳盈如，2014，資訊不實民事損害賠償之過失相抵－最高院 102 台上 1305 判決，台灣法學雜誌，251 期，頁 184。
2. 林國全，2015，財報不實之民事責任，月旦民商法雜誌，48 期，頁 29。
3. 林麗香，2016，財報不實損賠責任之計算－最高院 104 台上 225 判決，台灣法學雜誌，296 期，頁 182- 183。
4. 莊永丞，2005，證券交易法第二十條證券詐欺損害估算方法之省思，臺大法學論叢，34 卷 2 期，7- 13。
5. 葉新民，2009，論資本市場上因不實資訊而致投資人損害的賠償方法－以德國法為中心，中原財經法學，23 期，頁 48、159 以下。
6. 劉連煜，2006，財報不實之損害賠償責任：法制史上蜥蜴的復活？－證券交易法新增訂第二十條之一的評論，月旦民商法雜誌，11 期，頁 61、243。
7. 劉連煜，2013 財報不實案中有關證券持有人的舉證、過失比例責任及會計師事務所之連帶責任－台灣高等法院 101 年金上字第 7 號民事判決評釋，法令月刊，64 卷 12 期，頁 17。

21. 劉連煜，註 10 文亦即採此見解。

8. 劉連煜，2014 年 12 版，新證券交易法實例研習，頁 375，元照。
9. 劉連煜，2014，財報不實損害賠償之真實價格如何認定及投資人是否與有過失問題－最高法院 102 年台上字第 1294 號等民事判決研究，月旦法學雜誌，232 期，頁 240。

淺論區塊鏈之發展與趨勢

Exporing the Development and Trend of Blockchain

黃劭彥
國立中正大學會計與資訊科技學系教授

林有志
國立雲林科技大學會計學系副教授兼管理學院副院長

陳俊志
國立中正大學會計與資訊科技學系研究所博士生

郭博文
國立政治大學編審暨國立臺北商業大學企業管理系兼任助理教授

摘　要

2018 年係區塊鏈商用化的元年，區塊鏈正逐漸地改變政府、組織與產業樣貌，許多國家政府與企業已經積極投入，為了瞭解區塊鏈在產業之應用，實有必要針對區塊鏈概念及技術進行探討，並檢視可能面對的問題與挑戰，以協助政府與產業在相關領域的發展。

關鍵詞：區塊鏈、產業運用

Abstract

In the first year of commercialization of blockchain in 2018, the blockchain is gradually changing the appearance of government, organization and industry. Many governments and enterprises have been actively investing in order to understand the

industrial applications. It is necessary to explore the concept or technology of blockchain and examine the problems and challenges that may be faced to assist the development of government and industry in related fields.

Keywords：Blockchain , Industrial applications

壹、前言

2015年9月世界經濟論壇（World economic forum）報告指出，預期在2027年全球約有10%的GDP將儲存於區塊鏈技術之內，另《經濟學人》（The economist）2015年10月「The great chain of being sure about things」一文將區塊鏈稱為「確保萬物運作的巨大鎖鏈」。

我國為掌握網路科技發展與金融創新應用的國際趨勢，促成金融科技產業發展，金融監督管理委員會於2016年5月所提出的《金融科技發展策略白皮書》已將推廣區塊鏈技術，鼓勵業者投入應用研發列為11項重要施政目標之一。依據PwC 2016年全球金融科技調查報告資料顯示，在全球46國544位金融產業的CEO等高階主管中，有56%的受訪者表示，他們體認到區塊鏈技術的重要性，惟對於區塊鏈帶來的衝擊，有高達57%的受訪者表示不確定或不知該如何因應區塊鏈科技。即使在PwC 2017年調查1, 380金融服務與Fintech高階主管中，對於區塊鏈的瞭解程度僅有24%的受訪者認為非常熟悉（4%極度熟悉，20%非常熟悉），亦即有高達76%的金融服務與科技業主管認為並不是相當熟悉，然而卻有77%認為他們在2020年以前會於其一部分的生產體系或流程中導入區塊鏈技術，顯見區塊鏈技術及其未來潛力受各界高度重視，惟大家卻仍對它相當陌生。

本文首先介紹區塊鏈之定義與發展，其次整理區塊鏈之應用趨勢，最後提出區塊鏈發展之挑戰與風險，期望能讓各界能對區塊鏈技術及其應用與發展有進一步之認識。

貳、區塊鏈之定義與發展

一、比特幣與區塊鏈

比特幣(Bitcoin)是一種P 2P(Peer-to-Peer，點對點)形式的虛擬貨幣，採用密碼技術（又稱挖礦）來控制貨幣的生產和轉移，因此比特幣也被認為是一種電子加密網路貨幣（Cryptocurrency），由於其有特殊的隱密性，儼然成為全球電子交易和線上支付的媒介。區塊鏈（Blockchain）的起源主要始於比特幣的出現，係比特幣背後所代表的一項底層技術。提到比特幣與區塊鏈不能不提到一個神秘的虛擬人物－中本聰（Nakamoto Satoshi，日本媒體稱中本哲史）於2008年所發表的文章（該文亦被奉為比特幣白皮書）《比特幣：點對點的電子現金系統》（Bitcoin: a peer-to-peer electronic cash system），文中他提出了一個如何建立不需依賴第三方中介機構，即可在彼此不信任的狀況下、去中心化且願

意相互合作的電子現金交易系統。全文雖未直接提及 Blockchain 一詞，但卻不斷運用了區塊（ Block）、鏈（ Chain）、網路（Network）、節點（Node）等詞彙。

現代會計之父盧卡．帕喬利（ Luca Pacioli）於 15 世紀提出的複式簿記概念堪稱是會計界的偉大發明，人類開始使用「複式簿記法 」來記錄交易，並讓財務報表上的數字能夠被彼此瞭解與信任，包括近代的資本主義、國際貿易、全球金融等無不應運而生。所有交易透過第三方可信任的機構，並記錄於如銀行等金融中介機構的帳簿中，這些中介機構保存大家的交易記錄，全球金融離不開中心化的交易體系。然而區塊鏈以點對點的分散式網路系統，結合密碼學與時間戳（ Timestamps）等技術，透過數位簽章與一系列的機制，架構一個彼此在不信任的基礎下卻願意合作，且無須中介機構的新型態交易機制。

區塊鏈可以理解為一個超級大具時序性的網路帳簿或一個去中心化的資料庫，由所有參與的節點共同維護，這些節點也稱作礦工（ Miners），透過驗證交易可賺取比特幣。依據中本聰在論文中所提出之區塊鏈的運作機制，其流程為每一筆交易資訊會先透過區塊鏈系統廣播給各節點（ 礦工 ）進行驗證，再由每個節點替交易資訊蓋上時間戳，並計入區塊，此時所有節點需競爭解出雜湊（ Hash）函數（ SHA- 256），以爭取記帳權的方式來獲得比特幣作為獎勵；當某一節點解開了雜湊函數題，並經由其他節點核對無誤後，才得以將交易記錄至合法的區塊中，最新驗證過的區塊，會附加到先前已驗證過的區塊之後，形成區塊鏈帳冊（ Nakamoto 2008）。茲將區塊鏈運作流程簡述如下：

1. 交易產生：一筆新交易產生時，會先被廣播至區塊鏈網絡中的其它參與節點。
2. 各節點將數筆新交易放進區塊：每個節點會將數筆未驗證的交易 Hash 值搜集到區塊中，每個區塊可以包含數百筆或上千筆交易。
3. 決定由誰驗證這些交易：各節點進行工作量證明（Proof-of-work）的計算來決定誰可以驗證交易，由最快算出結果的節點來驗證交易，這就是取得共識的做法。
4. 取得驗證權的節點將區塊廣播給所有節點：最快完成工作量證明的節點，會將自己的區塊廣播給其他節點。
5. 各節點驗證並接上新區塊：其他節點會確認這個區塊所包含的交易是否有效，確認沒被重複花費且具有效數位簽章後，接受該區塊，此時區塊才正式接上區塊鏈，無法再竄改資料。
6. 完成交易驗證：所有節點一旦接受該區塊後，先前沒算完工作量證明工作的區塊會失效，各節點會重新建立一個區塊，繼續下一回工作量證明計算工作。

區塊鏈之特性歸納如下 (Iansiti and Lakhani 2017)：

1. 去中心化：區塊鏈透過各節點，共同維護一個大型分散式網路帳本，達到完全自主運作機制，不僅可避免以往中央資料庫有被入侵之風險，更可省

去中介機構，降低交易成本。

2. 安全性：區塊鏈分散式儲存之特性，資訊一旦寫入便無法修改，除非能掌控超過系統上 51% 節點才能更改數據，而這在目前幾乎不可能達到，亦即區塊鏈資訊無法被竄改。
3. 資訊透明：所有區塊鏈上的資訊，除了交易方的私有訊息加密之外，其餘的資訊可以在系統的公開平台做查詢，任何人都可以透過公開的介面查詢區塊鏈數據及開發相關之應用，因此整個系統資訊高度透明。
4. 獨立性：整個區塊鏈系統係基於協商一致的規範和協議（如比特幣的 Hash 演算法或其他各種演算法），不依賴第三方，所有節點能夠在系統內自動安全地驗證、進行資料交換，毋須任何人為的干預。
5. 可程式化：區塊鏈可以自動履行基本業務邏輯，建立智慧合約。
6. 成本與資產效率：區塊鏈可以催生低成本與高資產效率的商業模式。

區塊鏈依照其開放權限之不同可區分為公有鏈（Public blockchain）、私有鏈（Private blockchain）與聯盟鏈（Consortium blockchain）(Pilkington 2016)。公有鏈為完全開放及公開之區塊鏈，任何使用者皆可在公有鏈上讀取訊息、發送交易或驗證交易，是一去中心化之平台。雖然公有鏈具有完全去中心化、匿名且不可竄改的特性，惟仍可能有隱私或安全上之隱憂；私有鏈則是由某一組織或單位所創建的區塊鏈，該組織或單位掌控資訊的記錄權，在其他使用者沒有獲得權限之前，無法對該私有鏈上的任何區塊進行讀取、交易或寫入等動作，例如企業或政府的集中式資料庫，但私有鏈的規則及驗證主要由單一組織或單位執行，所以可能存在區塊被修改之風險；聯盟鏈則結合公有鏈及私有鏈的特性，是由多個組織或單位一起組成並共同運作與維護的區塊鏈，例如企業與企業間的共享資料庫，在聯盟鏈中的驗證工作主要是由預先選定的某些節點來執行，某些節點必須要有權限才能夠執行讀取或寫入，相較於私有鏈來說較可避免區塊被修改的風險，相較於公有鏈來說則較具隱私性 (Pilkington 2016; Underwood 2016; Dinh et al. 2017)。

2015 年 10 月《經濟學人》登載 < 信任的機器 >（The trust machine: the technology behind bitcoin could transform how the economy works）一文，強調區塊鏈是一個創造信任的機器，區塊鏈讓人們在互不信任，以及沒有中立的中介機構之情況下，能夠做到相互合作。區塊鏈技術是一種不依賴第三方，並通過自身分散式節點進行網路數據的存儲、驗證、傳遞和交流的一種技術。而從財務會計的角度來看，區塊鏈技術是一種分散式開放性去中心化的大型網路帳簿，任何人在任何時間都可以採用相同的技術標準加入自己的資訊，延伸區塊鏈，持續滿足各種需求帶來的資料記錄需求。基於上述觀點來看，區塊鏈可以說是創造一個大家都可以信任，且可以不斷延伸的具時序性網路帳簿及資料庫的超級機器。

二、區塊鏈之演進與發展

區塊鏈自 2008 年由中本聰提出迄今將近 10 年，一般而言可分成三個階段，其應

用也有所不同，茲將其演進說明如下：

1. 區塊鏈 1.0：比特幣

   比特幣開創了一個新的記帳方式，透過純粹交易者的交易，提供電腦硬體運算能力的礦工運算後加密，經所有區塊鏈上的人確認後連上區塊鏈，理論上資料將不可竄改並可追蹤。此時期主要應用為比特幣或其他數位貨幣的相關應用及去中心化的支付系統。

2. 區塊鏈 2.0：以太坊

   區塊鏈 2.0 的代表為以太坊（Ethereum），以太坊與比特幣相較主要係多了智能合約認證的區塊鏈技術，以太坊平台的使用者可自行開發自己想要的智能合約，許多區塊鏈公司透過此方法來發行自己的代幣。此時期區塊鏈被廣泛應用在各金融體系中，由於智能合約可用來記錄股權、版權、智慧財產權的交易，也可用於記錄醫療、證書、食品生產履歷等資訊，甚至可運用在旅遊住宿訂房、歌手發行專輯等，都可不需透過第三方中介機構。

3. 區塊鏈 3.0：整合應用

   區塊鏈 3.0 的代表相當廣泛，從 2.0 金融領域應用擴及到非金融領域之應用，並加入治理的概念（Swan 2015）。如 IOTA 即是一例，IOTA 是一種開放原始碼分散式帳簿（密碼貨幣），主要是提供物聯網上各機器之間資訊安全的通訊以及付款，並可連結實體生活、物聯網等。此外透過模組化結構，未來不只運用在智能合約而是連結到實體生活，不論會計、物流、房地產、保險等各領域將可利用區塊鏈技術進行革新，藉由開放原始碼，人人皆可創新創業，其應用能夠擴展到任何有需求的領域，進而擴及到整個社會。

參、區塊鏈之應用趨勢

區塊鏈之技術整合密碼學、數學、加密技術及經濟模型等，結合點對點的網路關係（P 2P），並採用分散式共識演算法，來解決傳統分散式資料庫的同步問題，可說是一套整合跨領域技術的基礎建設，目的係不需第三方機構協助驗證與對帳的條件之下，維護一套由多個參與者所組成網絡關係的資料庫。根據 RBC（the Royal Bank of Canada）2017 年的研究指出，虛擬貨幣、區塊鏈技術與去中心化是一個潛在價值高達 10 兆美元的生態系統，且這目標預計在 15 年內達成，未來區塊鏈會應用於任何領域，替人類生活帶來極大影響。以下係區塊鏈現行的應用情形與趨勢（徐明星等 2016 年）：

1. 醫療去中心化：醫療方面，區塊鏈最主要的應用是對個人醫療紀錄的保存，可理解為區塊鏈上的電子病歷。目前病歷是掌握在醫院手上的，患者自己並不掌握，所以病人就沒有辦法獲得自己的醫療紀錄和病史情況，如同銀行的帳看不到過往的交易紀錄一樣，對於未來的就醫會造成很大的困擾。惟如果可以用區塊鏈技術來進行保存，就有了個人醫療的歷史資料，未來看病或對自己的健康做規劃就有資料可供使用，而

這個資料真正的掌握者是患者自己，而不是某個醫院或協力廠商機構。另外，這些資料有很強的隱私性，使用區塊鏈技術也有助於保護患者隱私。這種應用具有去中心化的特性，更具開放性，用戶也更有自主性。它所實現的是一種新的組織資訊形態，每個人可掌握自己的資訊，而不需把資訊託管給某一個機構來保管。

2. 區塊鏈之基因定序檢測：當前公民獲取個人基因資料有兩個問題，其一為法律法規對於個人獲取基因資料的限制；再者，基因定序檢測需要大量計算資源，高昂之費用限制了產業進程。區塊鏈可解決基因定序檢測之問題，並透過全球分布的計算資源，低成本地完成基因定序檢測服務，並用私密金鑰保存測序數據規避了法律問題。經由數據分析，如果發現有潛在的高血壓、老年癡呆症，可以提前改變生活習慣以減少其發生機率。隨著區塊鏈基因定序檢測技術的成熟，針對大眾消費者的基因定序檢測服務將得到普及。區塊鏈還可應用到大數據領域，使其進入下一個世代，迎來真正的大數據時代，基因定序檢測就是區塊鏈推進大數據的一個典型案例。
3. 身分驗證：區塊鏈具有人人都可以查閱的特性，每個人都可以在任何一個有網路的地方，查詢區塊資訊，高度透明的特性也讓區塊鏈充滿吸引力。未來，可能不再需要身分證與戶口名簿，因為每個身分資訊都可以寫入區塊鏈裡，當需要驗證資訊的時候，只需要查閱即可找到。
4. 線上音樂：許多音樂人正選擇區塊鏈技術來提升線上音樂分享的公平性。依據《告示牌》（Billboard，美國音樂雜誌）2017年報導，目前有兩家公司正透過直接付款給藝術家和利用智慧合約來自動解決許可問題。在區塊鏈音樂串流平臺上，使用者可以直接付款給藝術家，而無須中間人插手。除了媒體音樂，還有人預想，將智慧合約作為歌曲清單的自主大腦，能夠更好地將歌曲背後的藝術家和創作者分類。
5. 數位藝術：數位藝術是區塊鏈加密技術顛覆性創新的另一個舞臺。數位藝術在區塊鏈行業的主要應用，是指利用區塊鏈技術來註冊任何形式的智慧財產權，或使數位藝術鑑證服務變得更加普遍，如合同公證。數位藝術可透過區塊鏈來保護線上圖片、照片或數位藝術作品的智慧財產權。
6. 人工智慧之區塊鏈：區塊鏈讓智慧設備在設定的時間進行自檢，會讓管理人員回到設備出故障的時間點去確定究竟什麼地方出了錯。應用區塊鏈技術可以遠端實施人工智慧軟體解決方案。如果一個設備有多個使用者，人工智慧區塊鏈也可幫助提高安全性，區塊鏈會讓使用各方共同約定設備狀態，並基於智慧合約中的語言編碼做決定。

7. 區塊鏈之智慧城市：生活於區塊鏈的智慧城市，我們可以為自己製造的麻煩情形付費，例如：因發生交通事故造成擁堵，可以支付給過往車輛延誤費用，促進社會往自律、高效自治的方向發展，還可以公開透明地為優良的服務及學校捐款或支付費用。
8. 區塊鏈之透明助學：區塊鏈的智慧合約有無數用途，智慧文化合約就是其中一種。如果有人資助孩子就學時，可以透過智慧合約自動確認學習進度，滿足學習合約後，自動觸發後續資金撥付給下一個學習模組。區塊鏈學習合約能夠使學習者與資助者之間完全以點對點方式進行協調，公開透明，對於雙方都是正向回饋，而學習合約將為慈善資助帶來革命性的突破。
9. 網路安全：雖然區塊鏈的系統是公開的，惟其核驗、發送等資料交流過程卻採用了先進的加密技術。這種技術不僅確保了資料的來源正確，也確保了資料在中間過程不被人攔截、更改。如果區塊鏈技術的應用更為廣泛，那麼其遭受駭客襲擊的機率也會下降，區塊鏈系統之所以能降低傳統網路安全風險，就是因為它解除了對中間人的需求。省去中間人不僅降低了駭客襲擊的潛在安全風險，也減少了貪腐產生的可能。
10. 預測市場：未來區塊鏈技術或將撼動整個研究、分析、諮詢和預測行業。線上募資平臺 Augur 希望能創建去中心化的預測平臺，這種服務類似博弈互換的服務。由於整個過程將被去中心化，Augur 平臺不僅會給用戶提供體育和股票博彩服務，還將提供選舉和自然災害博彩服務。這個想法實際上是超越了體育博彩的範疇，創造了一個「預測市場」。
11. 汽車租賃和銷售：目前信用卡與 Debit 金融卡支付機構 Visa 與提供 HYPERLINK "https://en.wikipedia.org/wiki/Electronic_signature" 電子簽名技術和 HYPERLINK "https://en.wikipedia.org/wiki/Digital_Transaction_Management" 數字交易管理服務的 DocuSign 公司宣布了一項合作計畫，利用區塊鏈技術為汽車租賃打造特定解決方案，以後汽車租賃只要「點、簽、開」三步即可完成。具體操作是：顧客選擇想要租賃的汽車，這筆交易就會上傳到區塊鏈的公共帳戶；然後，顧客在駕駛座簽署一份租賃協定和保險協定，區塊鏈便會即時將資訊上傳。不難想像，這種租賃模式或許未來也將應用於汽車銷售和汽車登記領域。
12. 智慧鎖：德國一個新創公司 Slock.it 正在研發區塊鏈技術的智慧鎖，並將鎖連接到互聯網，透過區塊鏈上的智慧合約對其進行控制。任何一個控制鎖的人都可以發放一把或多把私密金鑰，並對私密金鑰進行複雜的定制，設定鎖什麼時候啟用、具體什麼時候開啟等。透過這種方式，共享經濟能夠被進一步去中心化，將任何能被鎖起來的東西輕易租賃、分享

和出售。Slock.it 的概念更是超越了 Airbnb(提供短期出租房屋或房間的服務) 為使用者服務的範疇，想要進一步顛覆這種共享經濟，讓使用者能夠直接向一把鎖進行支付，然後打開；出租者也可以隨時更換私密金鑰的定制，讓整個體驗更為方便、安全。人們也可以透過使用這一技術進行自行車、密碼櫃的租賃等，甚至讓他人在自家門口替車充電，然後收取費用等。

肆、區塊鏈發展之挑戰與風險

現行學界與業界對分散式帳本與區塊鏈的應用多抱持著正向的看法，惟其還在發展初期，應用與發展上有許多未知且待解決的風險。

首先，新創技術的發展與應用成功率不高，且常遭遇到未知的挑戰，譬如比特幣的挖礦方式反而造成器材、設備、水電能源的競爭，不僅導致另一種中心化與進入障礙，也造成資源上的浪費，然目前仍有許多企業企圖採用其他科技方式解決與突破。

其次，目前分散帳本的技術尚未標準化，也難以達到一定的經濟規模。在應用上，多數還是由既有企業與政府主導分散式帳本系統，並傾向以聯盟或私有鏈方式建構，倘少數人掌握誰可以加入，且如金融應用需要匿名機制，可能無法解決原本的中心集權與透明化的問題。

此外，目前投入分散式帳本與區塊鏈技術應用的族群多是二、三十歲的年輕人，在顛覆式創新快速發展之下，要使既有政策制定與管制者了解並願意接受需要極大的溝通成本。例如，現行的共享單車、汽車、住宿為例，多數國家還在思考如何管理這類新創時，已經有不少新創想試圖以區塊鏈的去中心化來取代 Uber 這類的共享平台。由於未來無法確切掌握，政府應該結合新創，在其公共部門服務領域盡快開展小規模試驗，做中學過程，瞭解可能面對的問題並尋求解決的方法。

最後，區塊鏈的隱私特性，將會引發地下區塊鏈之發展，亦即如走私、藥品與槍枝販賣、賭博，以及如近期綁架電腦駭客要求比特幣付款等非法行為，均有誘因透過區塊鏈發展，這不僅是臺灣，也是未來國際間政府需要共同合作防範的問題。

伍、結論

過去沒有區塊鏈前，交易是一個中心化的世界，所有的交易必須有一個中介機構、交易所在中心做媒合，這些中心保存所有交易紀錄，讓全球經濟、金融體系可以運轉。而區塊鏈就是一種新的記帳方式，分散式帳本資料庫，每個帳本所記載的資料皆公開且無法被竄改，使用此技術最大的誘因即不用透過中介，可以 P 2P 直接進行交易節省手續費，而帳戶安全性則透過公鑰與私鑰兩組密碼讓使用者帳戶獲得保障。

未來政府部門將可能會是區塊鏈的最大使用者與受益者之一，區塊鏈將以去中心化、個性化、成本低、高效的特點顛覆傳統的政府治理模式，實現全新的、不同的政府管理模式與服務，經由充分利用區塊鏈優勢，能讓政府工作更高效，進而獲

得民眾的信賴。區塊鏈能利用其公開永久保存資料的優勢 — 共識驅動、公開審計、全球性、永久性 — 保存所有社會檔案、紀錄及歷史，供未來使用，成為全球性的資料庫，這將成為區塊鏈政府服務的基石。透過區塊鏈技術重新配置公共資源、提高政府效率、節約成本，促使財政惠及更多人、提高民眾基本收入水準、促進平等、提高民眾政治參與度，最終過渡到自治的經濟形態。不妨再設想一下更加久遠的未來，當區塊鏈所代表的思維範式，例如鳥群般的分散式協作、去中心化的模型，不僅應用於貨幣、資產的合約交易，而是直接作用於我們的大腦、神經元與認知，當人類大腦與電腦介面技術，配合區塊鏈網路共同展開，當人類與機器人記憶的提取、交易、存儲得以實現，當知識、靈感與創意的交互鏈條有序地形成，並不斷演進，那又將是何等的爆發式增長，何等恢宏壯麗的景象。

臺灣已錯失網路平台的機會，但區塊鏈將可讓臺灣企業不再得依附 Google、Amazon、Facebook、Apple、阿里巴巴等平台；且透過虛擬產品、服務、貨幣或資料等交易，實體貨品服務的全球貿易重要性將大幅下降，此亦可減緩臺灣目前遭受的國際邊緣化困境。目前臺灣的強項著重科技而非金融，而區塊鏈與智能合約的應用是設計給機器對機器的溝通，與人工智慧、物聯網、雲端運算具有密不可分的關係。倘就以 ICT 硬體研發製造為主的臺灣，若能把握發展可信任機器與產品發展的機會，掌握此優勢，並思考在區塊鏈下的創新商業服務，應該大有可為。

參考文獻

1. 金融監督管理委員會，2016，金融科技發展策略白皮書，台北：金融監督管理委員會。
2. 羅鈺珊，2017，分散式帳本與區塊鏈的應用現況與挑戰，經濟前瞻，173：pp. 79-84。
3. 徐明星、劉勇、段新星、郭大治，2016，區塊鏈革命：中介消失的未來，改寫商業規則，興起社會變革，經濟大洗牌，遠足文化出版。
4. Dinh, T. T. A., J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan,“Blockbench: A framework for analyzing private blockchains,”Proceedings of the 2017 ACM International Conference on Management of Data, p. 1085– 1100, 2017.
5. The Economist, "The great chain of being sure about things "p. 19- 22, 2015. 10. 31- 2015. 11. 6
6. The Economist ,"The trust machine " p. 11, 2015. 10. 31- 2015. 11. 6
7. J. P. Morgan CAZENOVE, Europe Equity Research，2016，Blockchain: A revolutionary technology too important to ignore.
8. KPMG，2016，2016 年 FinTech 100 金融科技創新者報告。
9. KPMG，2017，Global analysis of investment in finTech，The Pulse of FinTech Q 4 2017.
10. Iansiti, M., and Lakhani, K. R., 2017. The truth about blockchain. Harvard Business

Review, 95(1), pp. 118- 127.

11. Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.
12. Pilkington M., Blockchain Technology: Principles and Applications. Handbook of Research on Digital Transformations' edited by F. Xavier Olleros, and Majlinda Zhegu, Edward Elgar, 2016.
13. PwC, Global FinTech Report, 2016.
14. PwC, Global FinTech Report, 2017.
15. Swan M., 2015. Blockchain: Blueprint for a New Economy. Sebastopol, CA: O' Reilly Media.
16. Underwood, S., 2016. Blockchain beyond bitcoin, Communications of the ACM, 59(11), pp. 15- 17.
17. World Economic Forum, "Deep Shift Technology Tipping Points and Societal Impact Survey Report ", 2015. 9

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

Absence of Internal Control by Fraud Auditing and Forensic Accounting- Take KGI Bank's Foreign Exchange Trading Losses as an Example

林宜隆 I-Long Lin
元培醫事科技大學資訊管理系 教授
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

近期國內發生凱基銀行外匯交易員於 2018 年 4 月間違規超額炒匯事件，以 12. 6 億美元 (約新台幣 351 億) 操作加幣，最終導致 810 萬美元 (約新台幣 2. 4 億元) 的虧損。金融監督管理委員會 (以下簡稱金管會) 經過調查後，認為違法行為期間較長、影響層面大，「凱基銀前、中、後台都失靈 」，即為風險管理與內部控制制度之缺失，並重罰 800 萬元，並停止夜間交易 3 個月，該交易員也被命令解職。

因此藉由凱基銀行弊案，針對金融機構，可能面臨的風險管理和內部內稽缺失，從透過舞弊稽核、日常活動犯罪理論之 M-O-P 與鑑識會計探討，提供金融機構在面臨內部稽核有新的方法，減少公司內部控制缺失。

關鍵詞：內控內稽、舞弊稽核、日常活動犯罪理論之 M-O-P 、鑑識會計。

Abstract

Recently, the domestic foreign exchange traders of KGI Bank broke the excessive speculation in April 2018, operating the Canadian dollar for 1. 26 billion US dollars (about NT$ 35. 1 billion), which eventually led to a loss of 8. 1 million US dollars (about NT$ 240 million). After investigation, the Financial Supervision and Administration Commission (hereinafter referred to as the Financial Management Association) considered that the period of violations was long and the impact level was large. "KGI' s front, middle and back office failed," which is the lack of risk management and internal control systems. He was fined 8 million yuan and stopped trading for 3 months at night. The trader was also ordered to dismiss.

Therefore, with the disadvantages of the KGI Bank, the risk management and internal internal auditing that may be faced by financial institutions, from the discussion of MOP and forensic accounting through fraud audits and Routine Activity Theory, provide banking financial institutions with new internal audits new method, Reduce the lack of internal audit of the company.

Keywords: Internal control and internal audit, Fraud audit, Routine activity theory M-O-P, Forensic accounting.

壹、前言

統計金管會從 2013 年 ~ 2018 年 6 月對銀行業發出重大裁罰的案件總共 110 件，經統計違反內控目標之型態分別有：違反遵循目標有 87 件、違反營運目標有 65 件、違反報導目標有 27 件，裁罰案件內部稽核缺失違反內控目標之型態分類彙整表如表 1。然而這些違反都是可以透過鑑識會計的工作、流程方法將事前鑑識：安全防護機制及應變計畫；事中鑑識：處置及保留證據；事後鑑識：鑑定及資料復原，應用在內部稽核的手段中。數位證據鑑識不限於犯罪發生後，應該是把數位證據鑑識當作是犯罪預防的一項重要的工作。

表 1 裁罰案件內部稽核缺失違反內控目標之型態分類彙整表

項次	案件編號	裁罰對象	裁罰日期	違反內控目標之型態			裁罰金額
				型1	型2	型3	(新台幣)
一	1	凱基商業銀行	(1). 2018/6/29	■		■	800 萬元
二	2	華泰商業銀行	(1). 2018/6/26	■			300 萬元
三	3	京城商業銀行	(1). 2018/5/9		■		200 萬元
	4		(2). 2017/10/26			■	600 萬元
	5		(3). 2015/12/9			■	100 萬元
	6		(4). 2014/3/18			■	200 萬元
四	7	第一金融控股股份有限公司	(1). 2018/2/2		■		200 萬元
五	8	花旗(台灣)商業銀行	(1). 2018/2/1		■		850 萬元
	9		(2). 2014/7/8		■	■	400 萬元
六	10	臺灣銀行	(1). 2017/12/29	■	■		400 萬元
七	11	高雄銀行	(1). 2017/12/29	■	■		800 萬元
	12		(2). 2017/12/19	■			400 萬元
	13		(3). 2013/2/26			■	500 萬元
八	14	合作金庫商業銀行	(1). 2017/12/29	■	■		200 萬元
	15		(2). 2014/1/29			■	400 萬元
九	16	華南商業銀行	(1). 2017/12/29	■	■		200 萬元
	17		(2). 2016/11/8		■		800 萬元
	18		(3). 2016/3/8			■	300 萬元
十	19	臺灣中小企業銀行	(1). 2017/12/29	■	■		200 萬元
	20		(2). 2017/10/27		■		140 萬元
	21		(3). 2016/3/25			■	400 萬元
十一	22	兆豐國際商業銀行	(1). 2017/12/29	■	■		400 萬元
	23		(2). 2016/9/14			■	解除職務
	24		(3). 2016/9/14	■		■	1000 萬元
	25		(4). 2016/6/21			■	300 萬元
十二	26	第一商業銀行	(1). 2017/12/29	■	■		1000 萬元
	27		(2). 2017/11/7		■		140 萬元
	28		(3). 2017/1/24	■		■	200 萬元
	29		(4). 2016/9/12	■		■	1000 萬元
十三	30	臺灣土地銀行	(1). 2017/12/29	■	■		800 萬元
	31		(2). 2017/7/6	■		■	300 萬元
	32		(3). 2013/11/15			■	200 萬元
	33		(4). 2013/7/4			■	200 萬元
十四	34	遠東國際商業銀行	(1).2017/12/15	■		■	800 萬元
	35		(2).2017/1/5			■	1100 萬元
	36		(3). 2015/4/7			■	300 萬元
十五	37	中國信託金融控股股份有限公司	(1). 2017/12/5	■		■	1000 萬元
	38		(2). 2017/12/5	■		■	停止職務
	39		(3). 2017/12/5	■		■	停止職務
	40		(4). 2013/12/31			■	200 萬元
十六	41	中國信託商業銀行	(1). 2017/11/28	■			200 萬元
	42		(2). 2016/9/12	■		■	600 萬元
	43		(3). 2015/8/27	■		■	300 萬元
	44		(4). 2014/6/25	■		■	200 萬元
	45		(5). 2014/3/11	■	■	■	1000 萬元
	46		(6). 2013/11/14			■	200 萬元
	47		(7). 2013/8/22			■	400 萬元

十七	48	上海商業儲蓄銀行	(1). 2017/10/25	■			300 萬元
十八	49	台中商業銀行	(1). 2017/10/13	■			180 萬元
	50		(2). 2017/7/3	■		■	180 萬元
	51		(3). 2013/6/24			■	200 萬元
十九	52	聯邦商業銀行	(1). 2017/9/27	■			600 萬元
二十	53	永豐金融控股股份有限公司	(1). 2017/6/19	■	■	■	停止職務
	54		(2). 2017/6/19	■	■	■	解除職務
	55		(3). 2017/6/19	■	■	■	暫停業務
	56		(4). 2017/4/12	■	■	■	1000 萬元
二十一	57	台北富邦商業銀行	(1). 2017/6/13	■		■	100 萬元
	58		(2). 2016/9/12	■		■	600 萬元
	59		(3). 2016/5/11	■			200 萬元
	60		(4). 2014/6/25	■		■	400 萬元
二十二	61	臺灣新光商業銀行	(1). 2017/6/1	■		■	200 萬元
	62		(2). 2016/12/27			■	200 萬元
	63		(3). 2016/1/29	■		■	暫停業務
	64		(4). 2014/6/25	■		■	400 萬元
	65		(5). 2013/1/16			■	200 萬元
二十三	66	國泰世華商業銀行	(1). 2017/6/1	■		■	200 萬元
	67		(2). 2016/9/12	■		■	600 萬元
	68		(3). 2014/6/25	■		■	400 萬元
	69		(4). 2014/1/29			■	300 萬元
二十四	70	玉山商業銀行	(1). 2017/6/1	■	■	■	400 萬元
	71		(2). 2014/6/25	■			400 萬元
二十五	72	日盛國際商業銀行	(1). 2017/6/1	■		■	200 萬元
	73		(1). 2016/9/12	■		■	400 萬元
	74		(2). 2016/8/16	■		■	600 萬元
二十六	75	元大商業銀行	(1). 2017/6/1	■	■	■	400 萬元
	76		(1). 2016/9/12	■		■	400 萬元
二十七	77	大眾商業銀行	(1). 2017/6/1	■		■	400 萬元
	78		(2). 2016/9/12	■		■	暫停業務
	79		(3). 2014/6/25	■		■	400 萬元
	80		(4). 2013/10/3			■	400 萬元
二十八	81	安泰商業銀行	(1). 2017/5/2	■		■	1000 萬元
	82		(2). 2014/6/25	■		■	200 萬元
	83		(3). 2013/7/16		■	■	100 萬元
二十九	84	國際票券金融股份有限公司	(1). 2017/4/6	■		■	400 萬元
三十	85	王道商業銀行	(1). 2017/1/24	■		■	200 萬元
三十一	86	彰化商業銀行	(1). 2017/1/24			■	180 萬元
三十二	87	澳盛(台灣)商業銀行	(1). 2016/12/08	■		■	400 萬元
三十三	88	台新國際商業銀行	(1). 2016/12/2	■		■	800 萬元
	89		(2). 2014/6/25	■		■	400 萬元
	90		(3). 2013/7/9			■	600 萬元
三十四	91	星展(台灣)商業銀行	(1). 2016/12/1	■	■	■	1000 萬元
三十五	92	永豐商業銀行	(1). 2016/11/8		■	■	1000 萬元
	93		(2). 2016/9/12	■			暫停業務
	94		(3). 2015/6/9			■	400 萬元
	95		(4). 2014/5/1	■		■	停止業務
三十六	96	法商法國興業銀行	(1). 2016/3/10			■	200 萬元

三十七	97	板信商業銀行	(1). 2016/1/29	■		■	停止業務
	98		(2). 2013/6/21			■	200 萬元
三十八	99	新加坡商大華銀行	(1). 2015/10/5			■	200 萬元
三十九	100	香港商東亞銀行	(1). 2015/6/24			■	400 萬元
四十	101	法商法國巴黎銀行	(1). 2015/6/9			■	200 萬元
四十一	102	德商德意志銀行	(1). 2015/5/9			■	200 萬元
四十二	103	英商巴克萊銀行	(1). 2014/12/16			■	1200 萬元
四十三	104	臺灣永旺信用卡股份有限公司	(1). 2014/5/15	■	■	■	250 萬元
四十四	105	台灣工業銀行	(1). 2014/2/25			■	100 萬元
四十五	106	國寶人壽保險股份有限公司	(1). 2014/1/23			■	200 萬元
四十六	107	渣打國際商業銀行	(1). 2013/9/26			■	200 萬元
	108		(2). 2013/2/26			■	500 萬元
四十七	109	凱基證券股份有限公司	(1). 2013/7/22	■	■	■	200 萬元
四十八	110	中華開發工業銀行	(1). 2013/3/5			■	600 萬元

資料來源：參考邱靜宜，林宜隆，2015 研究方式，本研究整理

從舞弊看凱基銀行因為外匯交易損失而遭重罰，其中一個重要的因素存在著內部控制未有效執行的問題，建議全面升級全行 IT 資訊系統，運用資訊管理系統自動監控。

此本文以「凱基銀行外匯交易損失」為案例，銀行外匯交易流程：交易員透過對手銀行交易系下單→對手銀行接單後交易茲要回傳至交易員所屬銀行→銀行中後台系統收到資料計算是否符合限額等內控機制→不符合則發出警示至交易室 (搭配相關人力跟進確認違反內控行為更正消失) →交易室必須依據系統警示立即修正。

凱基銀柯姓交易員原本負責操作匯率，後來因績效好，在 106 年 9 月被調為「利率及信用交易科」交易員，並無辦理「匯率及商品交易科」交易權限。但凱基銀黃姓交易部門主管卻指定該員協助外匯科策略部份進行外匯交易，要他協助同仁交易匯率，最後居然變成他以其他同事的權限下單。柯姓交易員用自己與同事在銀行帳戶交易 1, 200 支（約 12. 6 億美元）的加幣，未料加幣兌美元在今年 2、3 月劇烈波動，該交易員操作方向錯誤，最後造成 810 萬元（約新台幣 2. 4 億）的損失。 (Phew, China time, 金款會裁罰案件) 將內部控制缺失的問題，導入國內學者林宜隆教授所提 MOP、數位鑑識 (鑑識會計) 之架構，進行方法及分析，有助減少銀行內部控制缺失的降低。

貳、文獻探討

一、內部稽核的意義及目標

依照本國「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。

第一項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。

第二項所稱之報導，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。
(金融監督管理委員會主管法規內容)

二、鑑識會計

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表 2、表 3。

表 2 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。

資料來源：林宜隆、林愫麗，2014

表 3 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)

資料來源：林宜隆、林愫麗，2014，本研究整理

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 1)，防弊措施可分為預防、偵測、調查、回應等四個階段。

圖 1 舞弊三歷程

資料來源：馬嘉應、蘇英婷，2007 年

四、舞弊三角理論與犯罪 MOP 理論

（一）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 2：

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。

（資料來源：高照，認識舞弊三角加強內部監管）

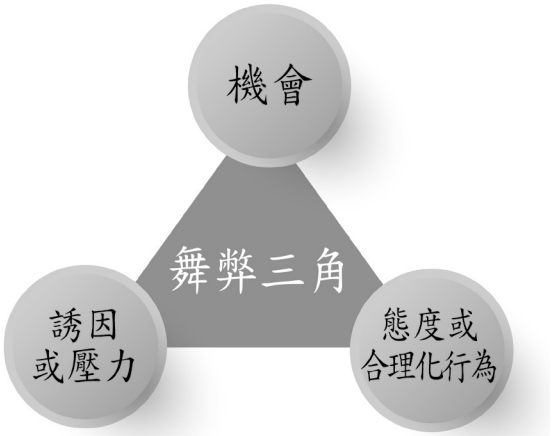


圖 2 舞弊三角理論圖

資料來源：林宜隆、林愫麗，2014

（二）日常活動犯罪理論之 M-O-P

日常活動理論為被害者學相關理論，由學者勞倫斯・柯恩（Lawrence E. Cohen）和馬可士・費爾森（Marcus Felson）在 1979 年所提出，該理論認為非法活動藉由日常活動的內涵，影響了犯罪發生的機會，因而影響「直接接觸掠奪性犯罪 」（Direct contactpredatory crime）的發生。所謂直接接觸掠奪性犯罪，乃指故意及明確的奪取、損害他人或他人財物之非法行為。而直接接觸之掠奪性犯罪，其發生的前提是犯罪者與被害者需在同一時空下產生接觸，接觸即促進了犯罪可能發生的機會。因此「機會」如何產生？在犯罪學理論裏，均偏重於犯罪者犯罪原因的探討，而日常活動理論跳出犯罪者為中心的傳統理論模式，而是以機會（Opportunity）來說明犯罪的發生，且認為若將有犯罪傾向者控制在一定的數量，但因社會環境的改變、人類活動型態發生變化，促成犯罪機會的增加，犯罪率仍會上升。

犯罪事件要發生必須有上述三要素在環境中相互作用，理論認為，直接接觸掠奪性違法行為的發生，需具備以下三要素：

1. 有動機之犯罪者（ Motivation，以字母 M 為代表 ）在場
   社會中原本即有相當數量的潛在犯罪人，若將該等人員控制在一定的數量，則犯罪率應可維持不變，但由於社會變遷結果，人類活動型態亦產生變化，直接造成犯罪機會的增加，提高犯罪率。
2. 合適的標的物（ Object，以字母 O 為代表 ）存在合適的標的物係以標的物的價值、可見性、對犯罪者的防禦性（Defense）而定，亦即犯罪者對標的物的需求決定其價值，及犯罪者可得知的標的物資訊、標的物自我的防禦能力；當標的物的價值愈大，可見性愈

高，防禦力愈低，其被侵害的可能性愈高。

3. 有能力遏止犯罪發生之抑制者不在場（Protection，以字母 P 為代表）有能力遏止犯罪發生之抑制者不在場泛指缺乏一般足以遏止犯罪發生的抑制力，並不單指警察人員，如商店為開放式之場地且面積寬廣，大多缺乏有效的監控，是發生竊盜的原因。

日常活動犯罪理論三要素動態模式（E 1 表示家庭環境，E 2 學校環境，E 3 社會環境），此理論中的三要素對於解釋為何會發生犯罪行為具有可操作性，有時亦稱為「犯罪基本三角（The basic crime triangle）」，此係學者林宜隆（2009）所提出之日常活動犯罪理論之 M-O-P。如圖 3。

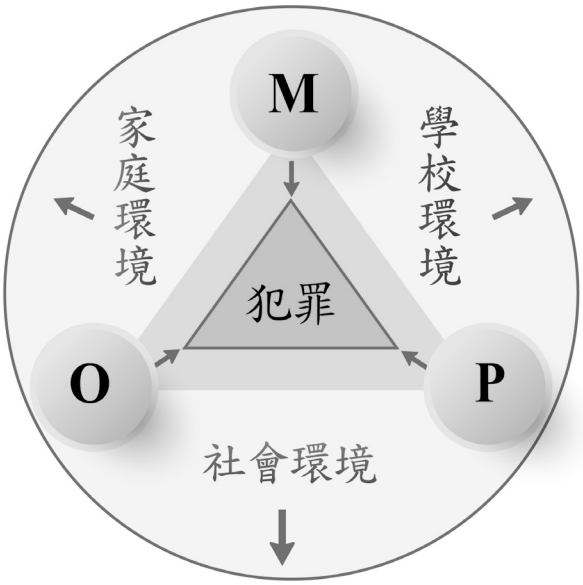


圖 3 日常活動犯罪理論之 M-O-P

資料來源：林宜隆、林慷麗，2014

（三）舞弊三角理論與犯罪 MOP 理論之分析比較

舞弊或犯罪的發生，均需要三大因素交互作用，在同一時間存在，犯罪才會發生。二者理論的基本要素名稱雖不同，但其內涵卻相同，例如：依據 Donald Cressey 舞弊三角理論的觀念，三大要素之一的「機會（Opportunities）」即是日常活動犯罪 理論之 M-O-P 中的 M（有能力及動機之犯罪者的在場），而「誘因 / 壓力（Incentive/pressure）」則是日常活動犯罪理論之 M-O-P 中的「O（合適標的物的存在）」，最後一個要素「行為合理化（Rationalization）」，為日常活動犯罪理論之 M-O-P 中的 P（有能力的抑制者不在場）。由此可知網路犯罪的基本理論，與舞弊偵查的理論所探討發生的原因均相仿。如表 4。

表 4 舞弊三角理論與犯罪 MOP 理論之比較

組成要素	舞弊三角理論	說明	犯罪MOP理論	說明	兩者比較	凱基銀行柯員案件解析
要素一	機會 (opportunities)	舞弊者可進行舞弊而又能掩飾不被發現或能逃避懲罰的時機。	有能力及動機之犯罪者的在場(M)	社會中原本即有相當數量的潛在犯罪人，隨社會變遷而增加。	均有潛在的犯罪者存在。	(一)未依個別交易員授權額度，於匯率及商品交易科策略部位設定交易上限及停損機制，致柯員進行之外匯交易，累計交易部位超逾該策略部位之授權額度。 (二)日間交易時間外無配置覆核人員以檢視交易員額度及監控交易等牽制控管機制。
要素二	誘因或壓力 (Incentive/ Pressure)	舞弊者從事舞弊活動的動機，包含財務與非財務性動機。	合適標的物的存在(O)	合適標的物其價值愈高，將引發犯罪的動機。	均屬犯案之動機。	有額外的bonus（獎金），交易員獲利越多，能拿到的獎金就愈多。
要素三	態度或行為合理化 (Rationalization)	為自身行為為合理化的說詞。	有能力的抑制者不在場(P)	沒人監看，讓犯罪者覺得罪行將不被發現。	犯罪者均為自身行為「找藉口」或「事後辯解」。	(一)後台作業單位就日/夜間交易時間外之交易，未能確實執行交易單據檢核、確認交易單流向及執行漏出交易單之作業程序。 (二)黃員擔任金融交易部主管，未能確實依貴行所定有關策略部位之管理原則，留存授權柯員操作策略部位之書面決策或授權軌跡；另對於超逾限額交易時之警示/超限通知，未覈實檢視及細究超限交易發生原因。

資料來源：林宜隆、林慷麗，2014、本研究整理

叁、凱基銀行外匯交易案件研究

凱基銀行 4 月 24 日爆出外匯柯姓交易員以 12. 6 億美元 (約新台幣 351 億) 操作加幣，最終導致 810 萬美元 (約新台幣 2. 4 億元) 的虧損。金管會經過調查後，認為違法行為期間較長、影響層面大，「凱基銀前、中、後台都失靈 」，重罰 800 萬元，並停止夜間交易 3 個月，該交易員也被命令解職。

一、數位證據鑑識標準作業程序 (DEFSOP)

案例分析的過程運用了學者林宜隆教授 What to do：發現了什麼線索；How to do：如何偵查；Why to do：由偵辦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。

數位證據鑑識標準作業程序 (Digital Evidence Forensic Standard Operation Procedure，DEFSOP)，透過標準作業流程 (SOP)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，供檢、警及調偵查人員在處理數位證據鑑識時的重要參考依據及標準化。如圖 4。(林宜隆 司法新聲 101 期)

數位證據的採證與鑑識程序的步驟為：

1. 事件辨別：事件辨別即情報蒐集與案件分析。其目的在於取得我們所需的資訊與相關資料，也在於預先了解案件的挑戰與可採取的因應之道。
2. 保存證據：進入現場後，最重要的便是保存證據。在調查之前，首先要確保得到允許後再開始調查。這一點，對於電腦犯罪案件中脆弱的數位

證據尤其重要，因為數位證據隨時都有可能因為鍵盤或滑鼠一按而改變。

3. 檢驗證據：在現場取得證據後，下一步就是如何去分析這些證據。
4. 案件分析與陳述：在取得證據並分析之後，就是如何將鑑識結果與嫌犯之間的關係進行分析。
5. 呈現結果：結果必須清楚的陳述。在探究證據的來源、成因與嫌犯的關係時，要去排除掉所有可能的替代解釋，來證明己方解釋的唯一解釋，方可明白確定無罪或有罪之假定。

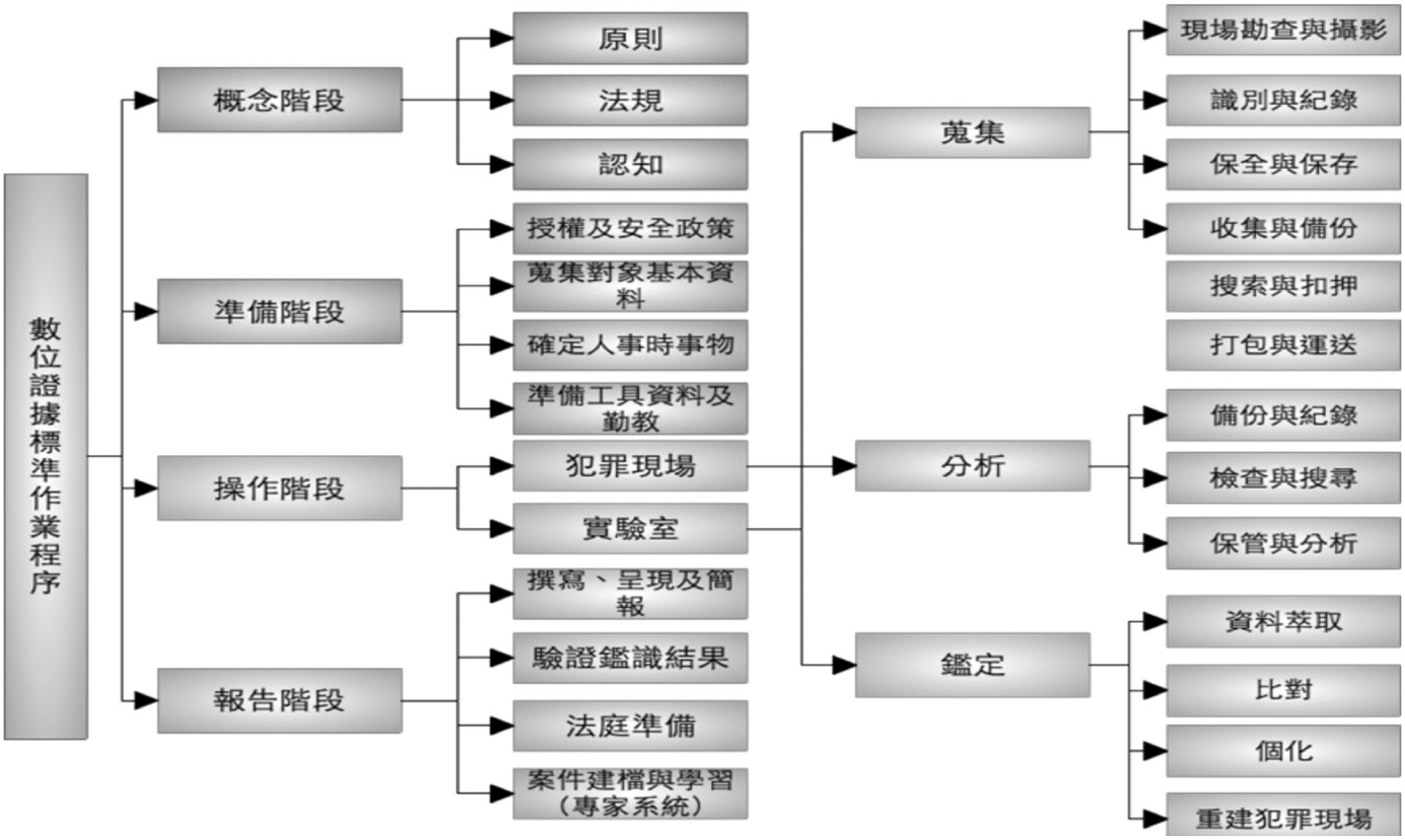


圖 4 數位鑑識標準作業程序

資料來源：林宜隆，2012

二、數位證據鑑識調查案例實證

凱基銀行外匯交易損失事證來看初步認定其為內部控制制度疏失，金管會也以行政裁罰凱基銀行，已於 107 年 6 月 27 日解除柯員之職務及停止副總經理黃員職務 3 個月，本案運用學者林宜隆教授提出的數位鑑識 (偵辦過程) 的方法分析，如圖 5。林宜隆、林悇麗 (2014) 鑑識會計應用於政府審計之研究的方法分析，如圖 6。

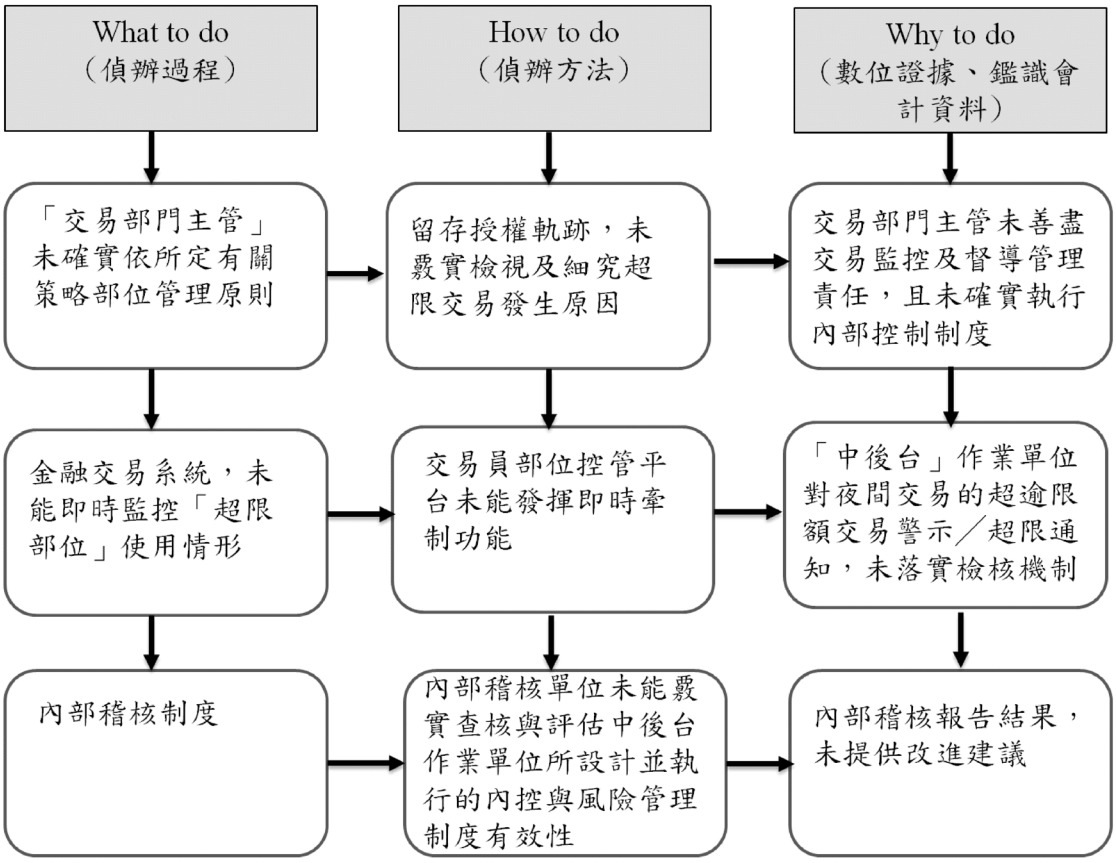


圖 5 數位鑑識（偵辦過程）的方法

資料來源：運用數位證據標準作業程序，本研究整理

圖 6 數位證據標準作業程序驗證圖

資料來源：運用數位證據標準作業程序，本研究整理

肆、結論

金管會的銀行重大裁罰案件，大多為銀行業的內部控制缺失導致，藉由數位鑑識的調查程序進行調查及數位證據標準作業程序，事前鑑識：安全防護機制及應變計畫；事中鑑識：處置及保留證據；事後鑑識：鑑

定及資料復原，提供銀行業的內部控制制度流程導入數位證據標準，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 (會計) 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。並透過建檔及學習的方式，來降低內部控制缺失的機會。數位證據鑑識不限於犯罪發生後，才來做數位證據鑑識，應該是把數位證據鑑識當作是犯罪預防的一項重要的工作。

參考文獻

1. 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。
2. 林宜隆，2009，網路犯罪理論與實務，台北，中央警察大學出版社。
3. 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。
4. 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，第一〇一期。
5. 林宜隆、林愫麗，2014，整合舞弊稽核與鑑識會計應用於政府會計之研究。
6. 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，32 期。
7. 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。
8. 高照，認識舞弊三角加強內部監管，https://www.verity.com.hk/images/news/ 2015/bamboo_aug 2015.pdf
9. 林宜隆，2012 年 1 月，「建構數位證據鑑識標準作業程序 」，司法新聲 101 期第 4 篇。
10. 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&dtable=Penalty
15. 金融監督管理委員會主管法規內容，https://law.fsc.gov.tw/law/LawContent.aspx?id=FL 049894

使用COBIT進行資訊組織設計

作者：Azha Zia-ur-Rehman
CISA · CRISC · CISM · ISO 27001 LA

譯者：陳政龍
CISA · CGEIT · PMP · CEH · ISO 9001,27001, 29100, 45001 LA

COBIT焦點｜2016年12月19日

資訊部門的組織架構通常是一系列變更、考驗、實驗和經營理念操縱的結果。它經常被調整成以適應或具有特許某些個人的情形。因此，資訊組織有時會被設計的很繁瑣，並且造成許多內部困擾、效率低下及成本過高的問題。

本文所描述的過程，是由許多重新設計與改造資訊組織的努力過程中所獲得的經驗而發展出來的。

第 1 步：選擇標準

資訊組織設計主要目標是在資訊投資中為利益關係者帶來價值。組織設計應遵循標準和良好實踐典範，以便最終的設計結果能易於辯護而且當中不存在爭議。首先需要從以下框架、標準和良好實踐典範中進行選擇：

- COBIT 5 - 確保資訊涵蓋各個面向的流程和任務。COBIT 5 還提供確保從利害關係人對於企業和資訊相關目標與所有促成因素要求一致性的必要結構。
- 資訊時代技能框架（ SFIA V 6）- 確保已包含所有必需的技能，並且反映在工作職務描述的設計中。
- ISO / IEC 38500:2015 詳細說明資訊治理面向的內容。
- ISO / IEC 20000:2011 詳細說明服務管理面向的內容。
- ISO / IEC 27001:2013 詳細介紹資訊安全面向的內容。

一些組織可能願意增加更多標準、實踐典範及當地的法規、守則或法律。在這方面非常有用的守則之一是 King III（即將成為 King IV），這是來自南非的公司治理守則。它可以在許多領域中用於設計強大的資訊治理系統。

在之前所列出的 5 個框架、標準和實踐典範中，前兩個不容忽視。至於剩餘的其他 3 個，高級管理階層可以自行決定是否列入考慮。

第 2 步：第一次迭代

功能組織的第一次迭代直接來自於 COBIT 5，並由以下功能元素組成：

- 董事會（BoD）

- 董事會的戰略執行委員會
- 指導委員會（向執行長報告）
- 執行長（CEO）
- 資訊長（CIO）
- 評估、指導與監督（EDM）領域
- 調整、規劃與組織（APO）領域
- 建立、獲得與建置（BAI）領域
- 交付、服務與支持（DSS）領域
- 監控、評價和評估（MEA）領域

圖 1 中列出了每項的輸出。

輸出到所有流程		
從關鍵實務	輸出描述	目的地
APO 13. 02	資訊安全風險處理計畫	所有 EDM；所有 APO；所有 BAI；所有 DSS；所有 MEA
輸出到所有治理流程		
從關鍵實務	輸出描述	目的地
EDM 01. 01	企業治理指導原則	所有 EDM；所有 APO；所有 BAI；所有 DSS；所有 MEA
EMD 01. 01	決策制定模型	所有 EDM
EDM 01. 01	授權階層	所有 EDM
EDM 01. 02	企業治理溝通	所有 EDM
EDM 01. 03	治理效益與績效的回饋	所有 EDM
輸出到所有管理流程		
從關鍵實務	輸出描述	目的地
APO 01. 01	溝通基本規則	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 01. 03	IT 相關策略	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 01. 04	IT 目標溝通	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 01. 07	流程改善機會	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 02. 06	信息包	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 11. 02	品質管理標準	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 11. 04	服務目標與度量指標的流程品質	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 11. 06	持續改進與良好實務的溝通	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 11. 06	良好實務範例的分享	所有 APO；所有 BAI；所有 DSS；所有 MEA
APO 11. 06	品質審查標竿結果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 01. 02	監督目標	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 01. 04	績效報告	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 01. 05	補救行動與任務	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 01	內部控制的監督與審查結果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 01	標竿與其他評估結果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 03	自評計畫與標準	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 03	自評的審查結果	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 04	控制缺失	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 04	補救措施	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 06	保證計畫	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 08	精簡範圍	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 08	審查結果保證	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 02. 08	審查報告保證	所有 APO；所有 BAI；所有 DSS；所有 MEA
MEA 03. 02	遵循性變更要求的溝通	所有 APO；所有 BAI；所有 DSS；所有 MEA

圖 1 - COBIT 5 過程的輸出

資料來源：ISACA、COBIT 5：促進流程與方法、圖 11、美國、2012

這些「責任（Accountabilitie）」和「職責（Responsibilitie）」列在 COBIT 5: 促成流程中的各種負責人、問責人、被諮詢者和被通知者（RACI）圖表中。董事會、戰略委員會、指導委員會和 C 字輩高階主管（CxOs）的各種「責任」和「職責」可以在現階段透過 RACI 圖表編制而成。在評估、指導與監督（EDM）領域各流程中列出的「活動」闡明了他們所必須參與的活動。

然後，可透過 SFIA V 6 來確保這些各別所需的所有技能都已經被各種利益相關者所擁有與具備。

在這一步驟結束時，董事會、戰略委員會、指導委員會和 C 字輩高階主管的責任、職責和活動即已經被決定和記錄確認了。

第 3 步：設計 [調整、規劃與組織（APO）]、[建立、獲得與建置（BAI）] 和 [交付、服務與支持（DSS）] 部分

APO、BAI 和 DSS 領域由許多子領域所構成（子領域在 COBIT 5 中稱為流程），在理想的情況下，這些子領域可以構成如圖 2、3 和 4 情況。

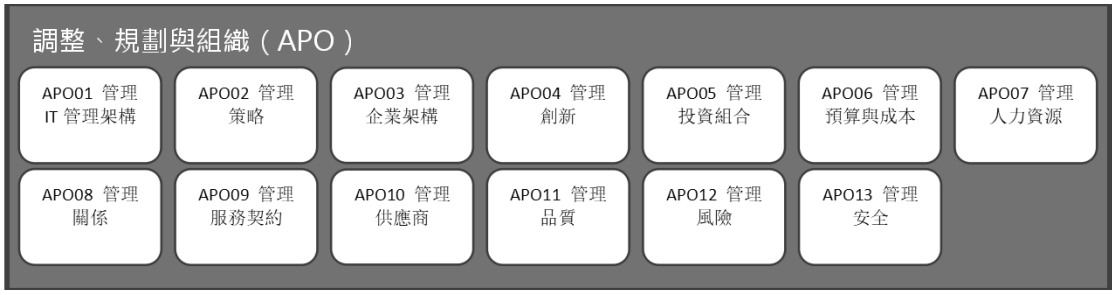


圖 2 – 調整、規劃與組織領域

資料來源：ISACA、COBIT 5、美國、2012

規劃時，可以考慮對於 COBIT 5 的這些流程進行分組，以減少部分的數量與減少人數。然而，在大型組織中，每個流程的本身可能就是一個部分，所以，以下只是對可能的分組方式提供建議：

- APO 01 和 APO 02 可以組合成為「資訊策略」。
- APO 03 和 APO 04 可合併為「資訊創新」。
- APO 05、APO 06 和 APO 07 理想下視為「資訊專案管理辦公室（PMO）」。
- APO 08、APO 09 和 APO 10 可以組合成為「服務級別管理」。
- APO 11 和 APO 12 可納入「資訊保證」項下。
- APO 13 構成「資訊安全（Information Security）」（而不是「資訊科技安全，IT Security」）。

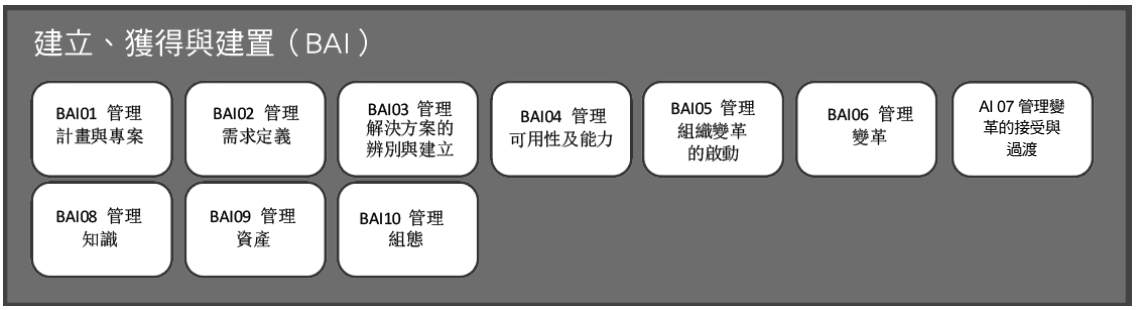


圖 3 - 建立、獲得與建置（BAI）領域

資料來源：ISACA、COBIT 5、美國、2012

- BAI 01 併入「資訊專案管理辦公室（PMO）」，當中並包含了 APO 05、APO 06 和 APO 07，這樣的規劃方式可運用在中型的資訊組織中。但企業在大規模進行內部開發的情形下也可設置為一個獨立的部分。
- BAI 02、BAI 03 和 BAI 04 在理想情況下應放入可稱為「應用程式設計」的部分。
- BAI 05、BAI 06 和 BAI 07 組合成為「資訊變更管理」。
- BAI 08、BAI 09 和 BAI 10 放入「資產和配置管理」項下。

圖 4 - 交付、服務與支持（DSS）領域

資料來源：ISACA、COBIT 5、美國、2012

- DSS 01 構成非常重要的「資訊營運」部分。
- DSS 02 和 DSS 03 合併為「事件和問題管理」。
- DSS 04 變成「持續性管理」部分。
- DSS 05 轉為「資訊科技安全（IT Security）」（而不是「資訊安全，Information Security」）。
- DSS 06 構成「控制管理」部分。

在小型資訊組織中，這些流程也可能會再考量做進一步的合併，但要注意的是，在所有列出的活動中應保持一些區隔，並且分配到所有的相關指標。

第 4 步：設計監控、評價和評估（MEA）部分

在中型和大型資訊組織設置時，最好也應設計具有資訊保證的部分，以確保資訊治理在資訊設置中完成。並且在規劃階段需要與內部稽核進行諮詢及與技術稽核進行技術性協商，同時也需要與企業的法遵部門進行包含規劃、實施和監控法

律、法規、標準和企業典範的做法。

而在規劃小型的資訊商店時，MEA 部分可以是內部稽核的一部分，也可以考量將內部稽核與企業法遵分別設置。

但是，無論如何，這些活動和相關指標均需在組織中要被完全的分配。

第 5 步：設計職位描述

設計好了組織結構後，接下來必須要對相應的職位進行工作描述規劃。職位描述可視為是一種活動與指標的組合，而這部分可透過 COBIT 5 及 SFIA V 6 所列出的活動資訊來進行建置。

所完成的職位描述必須包含下列內容：

- COBIT 5 中的所有活動都已分配。
- COBIT 5 中的所有相關指標均已分配。
- SFIA V 6 中列出的所有責任級別之所有技能都已被分配。

如有未分配的任何活動、相關指標和技能（包含在任何級別的責任）應列出管理，並說明未進行分配的合理性。

第 6 步：修改資訊流程

職位描述應該與資訊流程一致。因此，必須再對所有資訊流程進行一次檢視，並重新分配當中的職責以符合新的職位描述。

在進行資訊組織的設計和維護時，最好使用適當的工具來進行。當中所需要的功能包括有：

- 流程管理
- 企業架構
- 風險管理

許多治理、風險管理和法遵（GRC）的工具已經包含從使用它們進行組織設計的角度所需的評估和分析。GRC 工具必須具有風險管理及與企業架構相結合的強大流程管理功能。如果此套工具能支持成熟度評估，那麼它將會是更理想的工具。

本文中所描述的六個步驟過程已被用於設計過許多企業的資訊組織結構，無論企業的大小，它都是可以被執行的。這項資訊組織設計的活動在大型企業中可能需要數週時間才能完成，而在小型企業則可能約需要一週的時間。然而，在使用這種方法時，特別是需要確認已包含將 COBIT 5 中列出的活動與 SFIA V 6 中所描述不同責任級別間的技能保持一致。

任何組織調整都將與人有關，而且有時人們會反對這種建議的方法。只有在不影響職責分工要求的情況下才可將人的這個因素納入考量。

最後的建議是，資訊組織的設計需要按照理論來進行，然後再進行微調以終能符合企業的經營理念。

COBIT 5之風險架構：使IT風險管理變得有意義

作者：Syed Salman
CISA
譯者：諶家蘭
國立政治大學會計學系教授

COBIT焦點｜2017年6月12日

中東地區一家前四大專業服務公司被當地的一家大型零售銀行選中來協助實踐IT風險管理作業，從而可以具有成本效益的方式為企業創造價值。該銀行一直以來持續面臨一直增長且不斷改變的IT風險景況，由於高度依賴IT基礎架構及軟體應用系統向客戶提供有效率及效果的銀行服務體驗，董事會(BoD)的風險委員會(RC)決定，被列為最高優先順序的IT風險管理作業項目本銀行必須要落實。

需面對的基礎問題

風險長(CRO)與風險委員會(RC)均認為必須改進IT風險管理。以下方面需要特別注意：

- **分散之IT風險管理**—在過去幾年，企業中的不同單位（如：資訊安全部門、營運持續部門、IT治理部門、專案管理部門）於自身部門發展IT風險管理架構與IT風險登記表。除此之外，企業風險管理(ERM)單位擁有企業化的ERM架構，並促進包括IT部門在內的企業化風險評估作業。毋庸置疑，這導致了效率、效果皆差的IT風險管理。在許多情況下，企業內不同單位採用不同的風險管理架構和IT風險登記表，會導致同時以不同方式識別、評估和監控相同的風險，進而造成浪費資源；眾多不同的IT風險管理活動，將使IT部門的員工無法找到一個合適的風險管理方法與設計改善的計劃，並感到不知所措。
- **缺乏整合的風險報告**—該銀行中不同的IT風險登記表無法合併為一個，不同風險登記表的結構和風險評級方法完全不同。同時，不同部門有可能採用不同的風險因子，將所有IT風險整合到一個IT風險登記表中不止非常困難又耗時。因此，對於RC與CRO而言，IT風險管理活動既無法依賴又不有效。
- **風險文化**—該銀行受到行業文化的影響，鼓勵並強調服務提供，並在最短的時間內想出不同、創新的解決方案，故IT部門與該銀行整體並沒有

風險意識文化。

解決方法

RC 與 CRO 認為銀行應以單一且有系統的方式來控制 IT 風險，故委託一間值得信任且獨立，並致力於提供改善銀行 IT 風險管理的全新視野的專業服務公司。經討論，其一的解決辦法是採用最新的風險框架和四大會計事務所自身風險管理開發的系統來解決銀行面臨的問題。風險框架為由 ISACA 所發佈的 COBIT 5 風險架構，全面介紹了 IT 風險管理的主題，並提供有關風險的兩個觀點：風險功能觀點與風險管理觀點 (圖 1)。

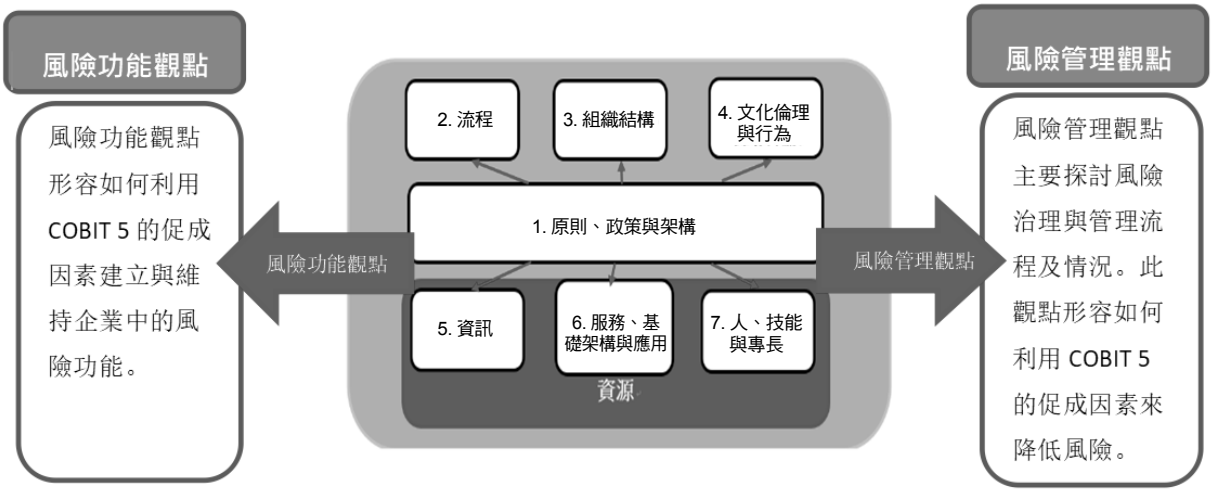


圖 1 風險的兩個觀點

風險功能觀點形容如何利用 COBIT 5 的促成因素建立及維持企業中的風險功能。風險管理觀點主要探討風險治理流程及情況，並且如何利用 COBIT 5 促成因素來降低風險。

除此之外，COBIT 5 風險架構詳述 7 個有助於 IT 風險管理的促成因素。

COBIT 5 風險架構所提出的促成因素簡列於下方 (圖 2)。

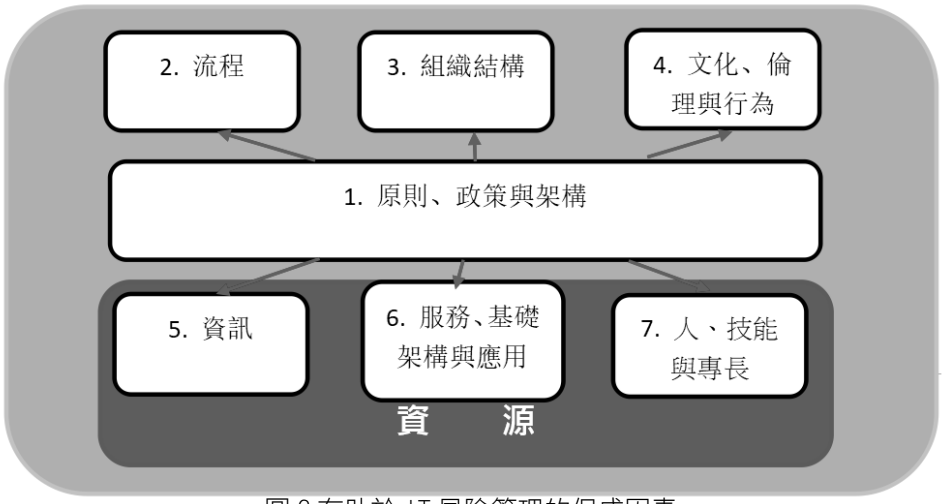


圖 2 有助於 IT 風險管理的促成因素

原則、政策與架構

COBIT 5 風險架構描述了企業於從事 IT 風險管理作業時應執行的原則，此原則提供企業於實施 IT 風險管理作業時有適合的基礎，企業可從了解並採用該原則中所提到的措施獲得效益。該原則包含：

- 與企業存在目的互相呼應
- 與企業風險管理緊密結合
- 平衡 IT 風險管理的成本與利益
- 提倡公平與公開的溝通模式
- 由高階人員負責並公佈消息
- 將實施風險管理當作日常活動的其中一環
- 持續進行

指引中描述企業在制定 IT 風險管理政策與有效性促成因素 (適用性、可覆性及分佈情況) 時建議考量並包含的元素。

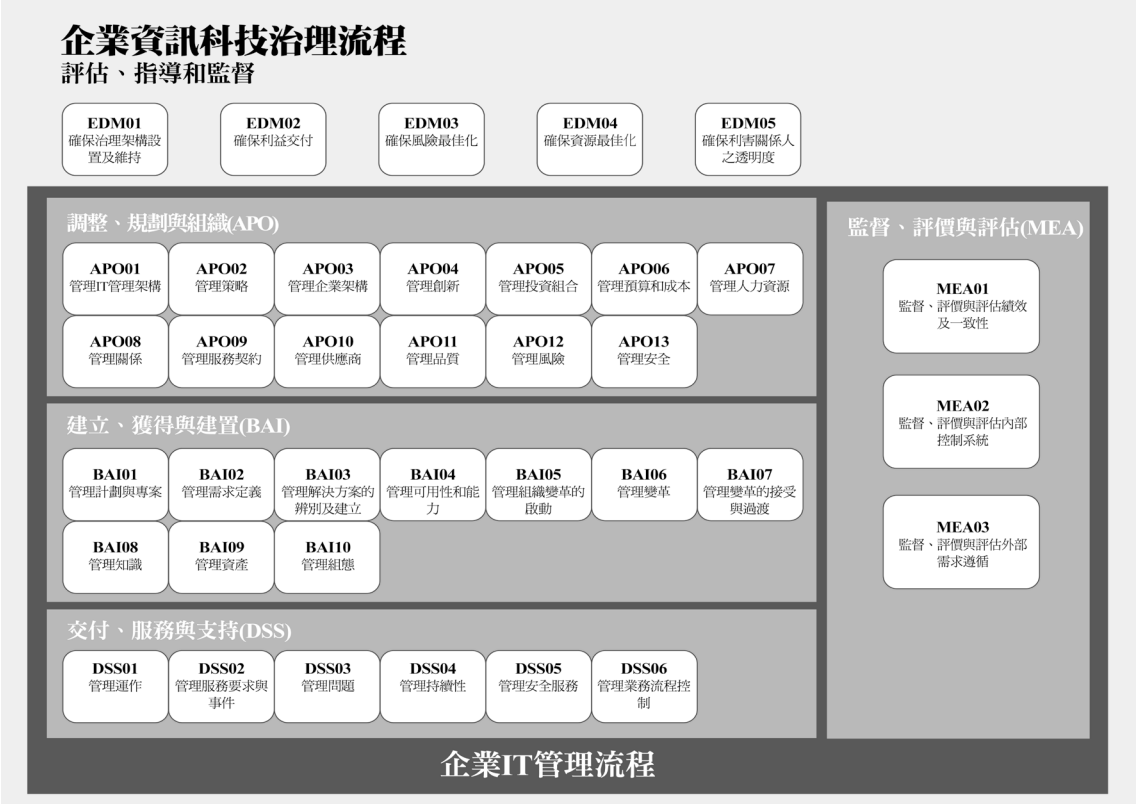
COBIT 5 風險架構提供一系列的風險政策並提供適當的描述，使專業人士可以更容易為他們所進行咨詢服務的企業設計出適合的政策。此外，COBIT 5 風險架構特地為 IT 風險管理框架保留一整段落，描述有效 IT 風險管理必須具備的所有元素。

在銀行業中，風險管理方式能幫助其處理「 風險管理工作分散各處 」及「 風險文化 」等問題。

流程

COBIT 5 風險架構針對重點風險流程提出了詳細的描述，核心風險流程 (圖 3) 包括：

- EDM 03 確認風險最佳化。
- APO 12 管理風險。



圖三 -COBIT 5 流程參考模型

來源 : ISACA, COBIT 5, USA, 2012

COBIT 5 詳細描述了每個流程，包括流程描述、流程目標、流程治理執行、流程管理執行，並建議企業使用關鍵績效指標（KPI）來衡量流程的績效。

此外，該出版品提供核心 IT 風險管理流程所需指引的支援流程，而該出版品不止提供了支援流程，也對流程所需指引進行描述。

針對該銀行面臨的問題，上述促成因素可解決「缺乏整合報告」的問題。

組織結構

COBIT 5 為進行 IT 風險管理時該採用的關鍵結構或角色提供了簡潔的指引和描述。此外，「三道防線」模型（圖 4）中呈現此結構，以便更容易理解在組織中應該如何配置該關鍵結構或角色。

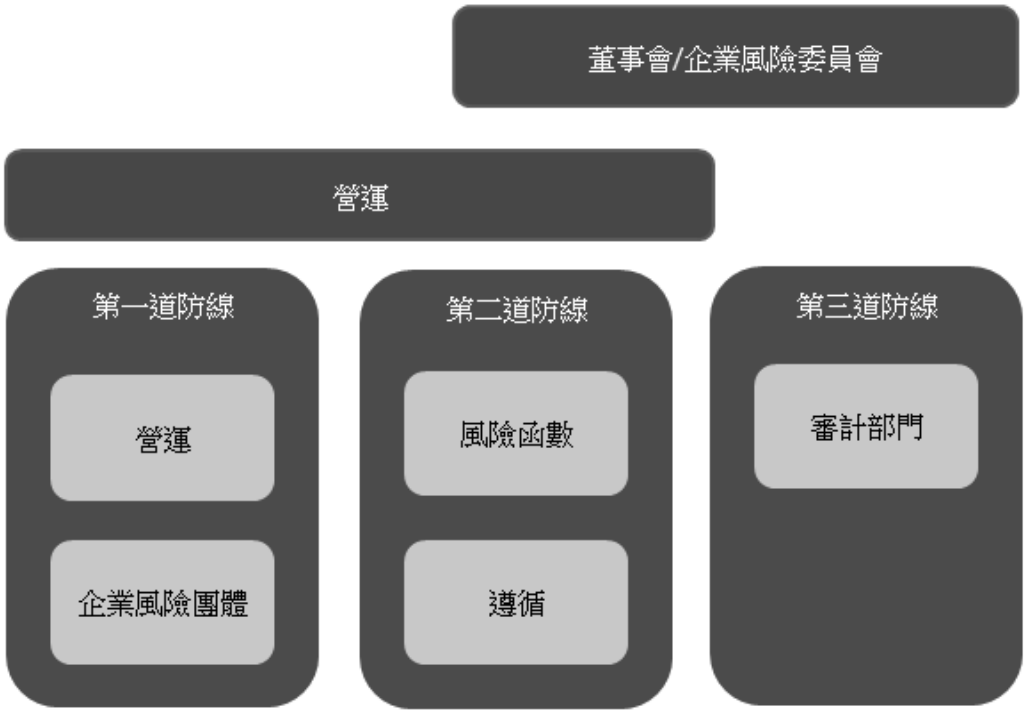
應採用之結構 / 角色包括 :

- ERM 委員會
- 企業風險團體
- 風險功能
- 審計部門
- 法令遵循部門

與 IT 風險管理有關的支援結構 / 角色，包括：

- 董事會 (BoD)
- 執行長 (CEO)
- 資訊長 (CIO)/ 技術長 (CTO)
- 資訊安全長 (CISO)
- 營運持續計畫經理

針對該銀行面臨的問題，COBIT 5 促成因素可以幫助解決「IT 風險管理工作分散化」的問題。



圖四－防禦風險的防線

來源 : ISACA, COBIT 5 for Risk, USA, 2013

文化、倫理與行為

促成因素「文化、倫理與行為」目的為於企業中建立、維持有效率及效果的風險管理時，確定企業整體所需的相關行為和文化要素，並有助於在企業的各個層面建立和維護風險意識文化。

理想的行為按照企業內部的三個層次進行分類：

- 一般（全企業）
- 風險專業人士
- 管理階層

對於每個行為，COBIT 5 分別描述了結果。

關於銀行面臨的問題，此促成因素可以幫助解決「風險文化」問題。

資訊

促成因素「資訊」描述了在企業中建立、維持有效率及效果的風險管理所需的所有資訊項目，其中列出了許多構成企業風險相關來源的資訊項目，並對其進行了定義和描述，其中的項目包括：

- 風險概況
- 風險溝通計畫
- 風險報告
- 風險地圖
- 風險偏好
- 風險承受能力
- 風險分類
- 風險和控制活動矩陣

針對銀行面臨的問題，該促成因素可以幫助解決「IT 風險管理工作分散」和「整合的風險管理報告缺乏」等問題。

服務、基礎架構與應用

促成因素「服務、基礎架構與應用」辨認和描述在企業建立、維持有效率及效果風險管理時，所需的所有服務、基礎架構和應用程序。

具體描述的項目包括：

- 公司治理、風險和法令遵循（GRC）工具
- 風險溝通 / 報告工具
- 事件管理服務

針對該銀行面臨的問題，此促成因素可以幫助解決「IT 風險管理工作分散」和「整合的風險管理報告缺乏」等問題。

人、技能與專長

此促成因素提供了有關人的技能及專長如何指導企業風險治理和管理，具體技能和能力包括：

- 風險專業知識
- 組織和企業意識
- 批判性思維
- 分析能力

針對該銀行所面臨的問題，此促成因素可以幫助建立所需的技能和能力，以解決面臨的每一個問題。

結論

企業通過採用 COBIT 5 風險架構中描述的七個促成因素可以解決本文所述的基本問題，當專業人員欲在其組織中建立有效率及效果的 IT 風險管理能力時，此出版品將

十分具參考價值。

COBIT 5 風險架構辨認和解釋 IT 風險管理各個組成部分，將之整理並系統化，幫助從業人員找到有關 IT 風險管理相關事宜的指引。更重要的是，該出版品允許 IT 風險管理從業人員通過參考 ISACA(一個享有盛名的世界知名機構) 的權威指導來讓所有利益相關者接受並取得共識，以利 IT 風險管理的推動與改變。

如何運用COBIT 5評估資訊流程及相關安控標準的遵循-以彩券業為例

作者：

Ioannis Panopoulos
CISA, CRISC, CGEIT, CSXF, ISO 27001 LA

Maria Melliou
CISA, CAML, CCO, CIA, CRMA, ISO 27001 LA

譯者：

黃誌緯
安永聯合會計師事務所 資深經理

陳冠穎
安永聯合會計師事務所 顧問

呂良仁
安永聯合會計師事務所 顧問

COBIT焦點｜2017年10月16日

近年來隨著新興資訊科技應用的蓬勃發展，資訊科技風險控管、資訊科技價值創造與治理等新興議題拓展了電腦稽核的應用與關注領域。

為了有效的執行電腦稽核並評估資訊流程能力及相關控制，本文以彩券業為例，描述如何使用 COBIT 5 流程模型並配合 GRC(公司治理、風險控管以及法規遵循) 平台，可以讓公司資訊安全流程與全球彩券行業標準 (WLA-SCS: 2016) 一致，讓組織資訊流程功能的審計、評估和呈現變得更有效率。

關鍵詞：COBIT 5、WLA Security Control Standard、ISO 27001、彩券

壹、前言

歐洲最大博弈業者的內部稽核團隊導入以雲端技術為基礎的 GRC(公司治理、風險控管

以及法規遵循) 平台，以提升審計工作文件的品質及與其他審計服務團隊 (如：法遵、風控、資安) 工作效率及協作。MetricStream[1]被選為執行此次 GRC 平台導入專案的夥伴，該平台提供了快速評估流程、風險和控制的有效性和效率的功能。

為了評估資訊流程能力和相關控制的設計與執行之有效性，該業者選擇 COBIT 5 流程模型並上傳到 GRC 平台流程，COBIT 流程模型可輕鬆比對到國際標準組織 / 國際電工委員會 (ISO/IEC) 的 ISO/IEC 27001: 2013 資訊安全標準中，該標準已納入彩券公司廣泛採用的一項標準：WLA 安全控制標準 (WLA-SCS: 2016)[2]。因此，使用此自動化審計管理系統和標準化控制框架，可以輕鬆實現與全球彩券行業一致的標準，且可重複的評估組織資訊流程的效率、效果、成熟度和法遵準備情況。

一、世界彩券協會 (World Lottery Association, WLA) 安全控制標準定義彩券的安全性，對於維護公眾對彩券遊戲的信心和信任至關重要。因此，彩券機構必須發展並維護一個可見及可證明的安全環境，以實現和維持公眾對其業務的信心。

WLA-SCS 是彩券業唯一國際公認的安全標準。WLA-SCS 結合全面的資訊安全管理基準，將資訊安全管理的國際領先標準 ISO / IEC 27001: 2013 與代表當前最佳實踐的其他彩券專用安全控制相結合。WLA-SCS 旨在幫助全球的彩券部門根據公認的最佳實踐獲得一定程度的安全控制，以加強對彩券業務完整性的依賴。WLA-SCS 規定了有效的安全管理結構所需的做法，通過該做法，抽獎業務可以保持對其安全操作至關重要的資訊之完整性、可用性和機密性。

二、實施步驟

為了實現這一目標，計畫實施以下步驟：

步驟一、認識在企業資訊環境中運行的 COBIT 5 流程。

步驟二、將 COBIT 5 流程比對到 WLA-SCS: 2016 和 ISO/IEC 27001: 2013 的流程和控制。

步驟三、在 GRC 平台上使用檢查表及調查評估 COBIT 5 流程、WLA-SCS: 2016 和 ISO/IEC 27001: 2013 控制。

步驟四、將結果上傳到資料視覺化平台並產出報告。

1. 認識在企業資訊環境中運行的 COBIT 5 流程。

在大規模商業轉型的背景下，內部稽核促進了整個組織內運行的企業流程 (包括資訊流程) 的收集和索引。COBIT 5 流程模型被用作識別組織資訊核心流程的基礎模型，無論資訊核心流程是外包還是自行營運。技術長 (CTO) 會與其團隊進行討論，以確定最重要的資訊流程包含在企業流程模型中。該實驗的結果顯示，絕大多數 COBIT 5 流程被辨認為適用並已上傳到 GRC 平台。

此外，在這一步驟中，最初的努力是評估過程如何影響資訊的機密性、完整性和可用性，並估算所處理資訊的過程「復原時間目標 (RTO)」和「復

原點目標（RPO）」，以便反映在業務連續性和災難恢復計劃中。

2. 將COBIT 5流程比對到WLA-SCS: 2016和ISO/IEC 27001: 2013的流程和控制。

在辨認出適用的COBIT 5流程後，下一步就是將這些流程比對到一個普遍接受的博弈規範框架。

如前所述，WLA-SCS是全球彩券公司廣泛採用的標準。 WLA-SCS標準描述了一般安全控制（包含ISO / IEC 27001所規範）以及所提供遊戲的安全性有關的特定控制。使用COBIT 5進行資訊安全（COBIT 5 for Information Security），尤其是參考表格“比對COBIT 5之資訊安全控制與相關準則（Mapping of COBIT 5 for Information Security to Related Standards）”，可以輕鬆將COBIT 5流程比對到ISO / IEC 27001，從而涵蓋WLA-SCS: 2016的資訊安全要求。圖1闡明了COBIT 5和WLA-SCS: 2016之間的相互關係，包括可以分別評估哪些領域。

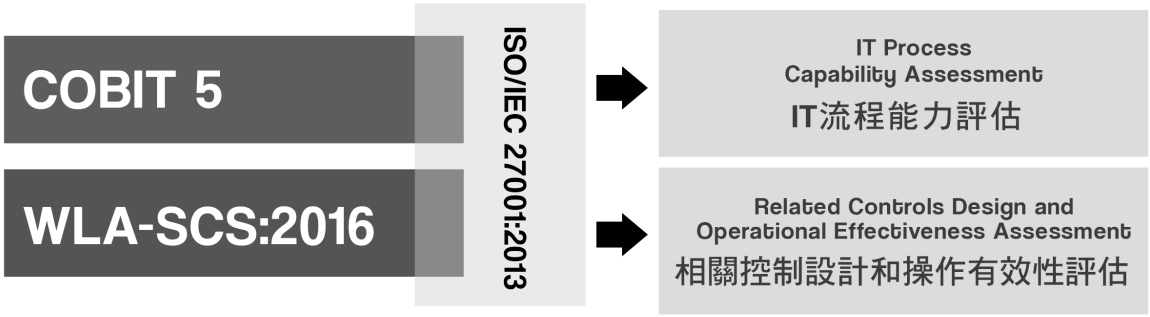


圖1: COBIT 5及WLA-SCS: 2016之關聯

在圖 2 中，介紹了其他標準和框架的 COBIT 5 覆蓋範圍，包括 ISO / IEC 27000 系列。

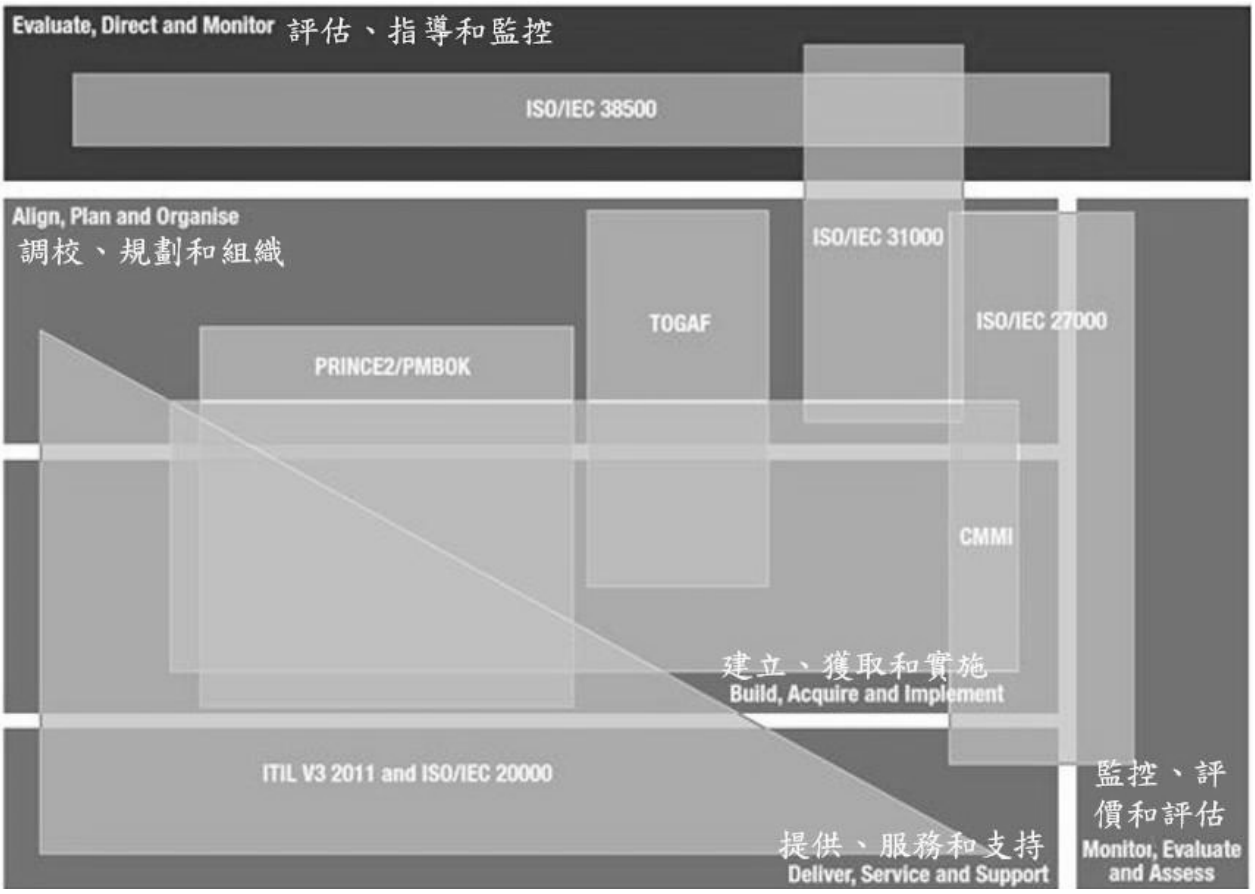


圖 2：比對 COBIT 5 及 ISO/IEC 27000 系列

資料來源：ISACA, COBIT 5 for Information Security, USA, 2012

3. 在 GRC 平台上使用檢查表及調查評估 COBIT 5 流程、WLA-SCS: 2016 和 ISO/IEC 27001: 2013 控制。

為評估圖 1 所示的區域，採用了以下方法：

(1) 對於 COBIT 5 流程，採用了 ISACA 的流程評估模型 (PAM)，其包含流程評估模型，評估指南及 PAM 工具包。

(2) 對於 ISO/IEC 27001: 2013 標準，則採用 ISO/IEC 27002: 2013 標準中所提到的控制點及控制目標。

(3) 對於 WLA-SCS，採用 WLA-SCS 或相關指引 (例如：網路博弈資訊安全指南、體育博弈指南) 所提及的控制目標。

為了便於評估 COBIT 5 流程、WLA-SCS: 2016 和 ISO/IEC 27001: 2013 控制，使用 GRC 平台提供了一套機制 (如調查和檢查表 [圖 3]) 和標準化流程。

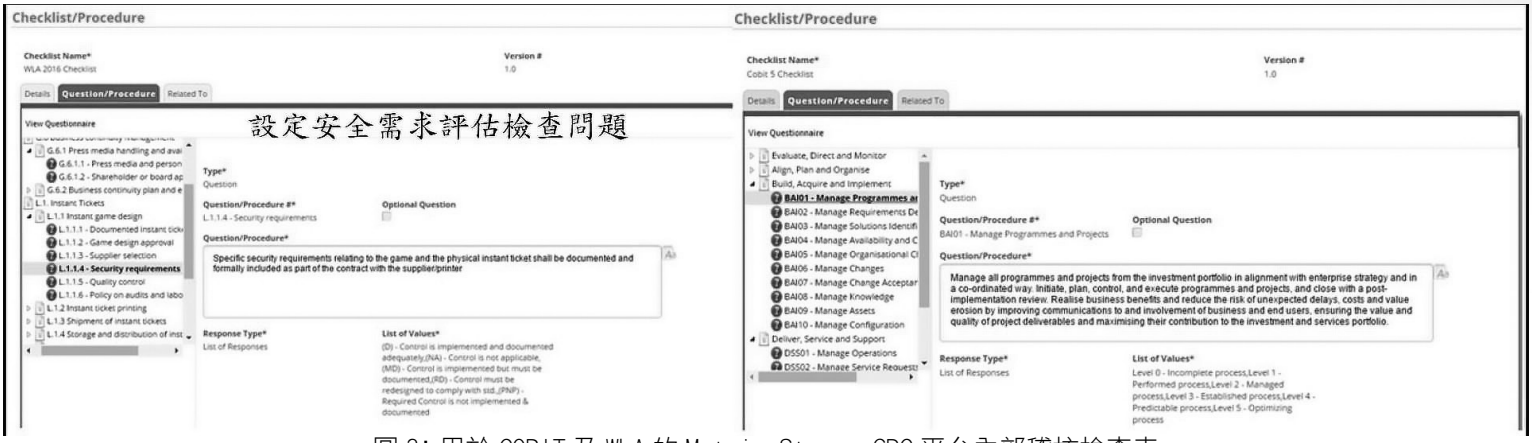


圖 3：用於 COBIT 及 WLA 的 Metric Stream GRC 平台內部稽核檢查表

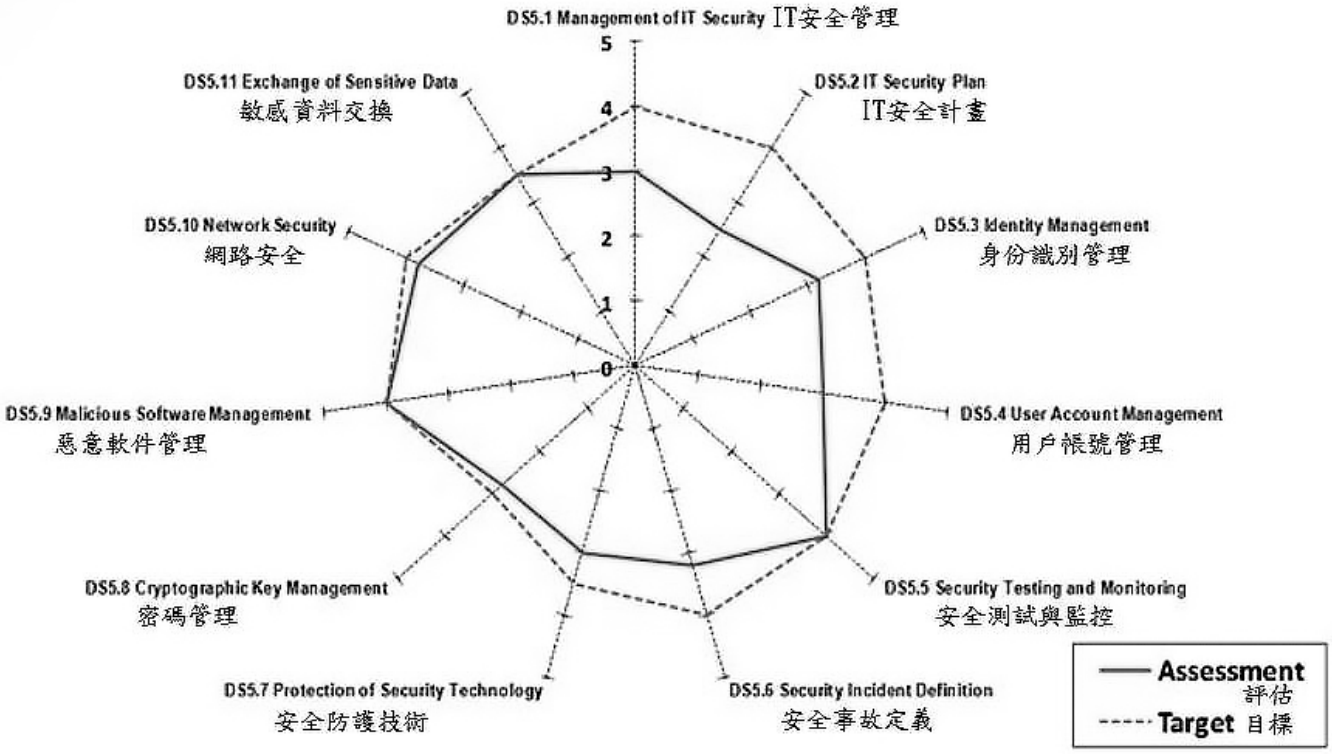
在整個審計生命週期中，調查和檢查表被用於很多步驟。在編製稽核計劃之後，特別是在規劃階段，調查用於要求業務團隊自行評估查核範圍涉及的資訊流程成熟度水平。在實地工作階段，依照檢查表執行具體任務，以測試查核範圍流程、風險和相關控制設計及執行之有效性。最後，在稽核工作結束之前，由稽核人員測試的流程將被評估其剩餘風險和成熟度水平。

4. 將結果上傳到資料視覺化平台並產出報告。

如前所述，COBIT 5、ISO/IEC 27001 及 WLA-SCS 之間存在著關聯性。同樣在 COBIT 5 中，企業目標和資訊相關目標[3]、以及資訊相關目標和資訊相關流程之間也有詳細的對應。[4]

因此，執行步驟三所描述的評估後，結果會被上傳至資料視覺化平台（例如：SAS Visual Analytics, Excel Power BI）。關於先前描述的範圍之當前及目標狀態以及資訊治理、資訊安全及彩券相關之控制都會透過儀表板的使用（圖 4）進行了可視化呈現，以向相關利益相關人提供有用的見解。

圖 4：蛛網圖：COBIT 流程評估及目標值的樣本



貳、結論

使用 COBIT 5 框架以及 ISO 27001 和 WLA-SCS 標準，可以為組織各級之間的資訊流程建立一個通用語言，並為評估這些流程的能力提供標準化的方法。此外，通過使用 GRC 平台和資料可視化工具，資訊流程功能的審計、評估和呈現變得更加有效率。關鍵之處在於，在這種持續的努力中，採取了小而精，而非大而複雜的步驟。

注釋

1. MetricStream, Internal Audit Management Application company
2. World Lottery Association, WLA Security Control Standard: 2016 (WLA-SCS: 2016), 2016
3. ISACA, COBIT 5, USA, 2012
4. Ibid., Appendix C

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。秘書長由黃涼澤擔任。
- 2002 年 9 月由蔡蜂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。秘書長由黃涼澤擔任。
- 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。秘書長由黃涼澤續任。
- 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。秘書長由黃涼澤續任。
- 2018 年 9 月由張紹斌續任第十三屆理事長。副理事長由蒲樹盛擔任。秘書長由黃涼澤續任。

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 (CGEIT) 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。

June-September 2018 Certification Exam Passers

ISACA Taiwan Chapter

	Exam Type	ID No.	Name	Top 3
1	CISA	341236	Hsin-Ju Chen	
2	CISA	877616	Yu-Mei Lee	
3	CISA	1126201	Hui-Ling Chiu	
4	CISA	1127867	Chien Ho Lu	No.1
5	CISA	1128414	Meng-Shu Hsieh	
6	CISA	1144892	Chang-Huei Liou	No.3
7	CISA	1145558	Pei-Chia Chen	
8	CISA	1147749	Chin-Yuan Yi	No.1
9	CISA	1152016	Wentz Wu	No.2
10	CISA	1166709	Cang-Lang Lin	
1	CISM	1148048	Hong-Kuo Chuang	No.2
2	CISM	1152016	Wentz Wu	No.1
1	CRISC	1010625	Te-Yin Su	No.2
2	CRISC	1043758	Wen-Liang Sun	No.3
3	CRISC	1152016	Wentz Wu	No.1
1	CGEIT	1049270	Yao-Hsun Chen	No.1

※ 以上資料來源： ISACA總會201809更新。

2019 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	**4/15-19** **9/11-12**、**18-20**	NT$ 30,000
	CISA 國際電腦稽核師認證研習班_假日班	30	**3/9**、**16**、**23**、**30**、**4/13** **8/3**、**10**、**17**、**24**、**31**	NT$ 30,000
	CISM 國際資訊安全經理人認證研習班_假日班	18	**4/20**、**27**、**5/4** **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	**5/11**、**18**、**25** **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	**1/21-25**、**2/18-19, 25-27**、**3/18-22**、**4/22-26**、**5/20-24**、**6/17-21**、**7/18-19, 24-26**、**8/12-16**、**9/16-20**、**11/11-15** **12/9-13** 假日班：**10/17-19, 25-26** 高雄班：**4/22-26**、**9/16-20**	NT$ 53,000
	ISO 27001:2013 資訊安全管理系統 內部稽核員訓練課程	16	**5/13-14**、**9/23-24**	NT$ 21,000
	ISO 27001:2013 資訊安全管理系統 建置實務課程	24	**5/13-15**、**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	**2/18-22**、**5/6-10**、**8/12-16**、**11/11-15** 假日班：**6/13-15, 21-22** 高雄班：**9/2-6**	NT$ 55,000
	ISO 22301:2012 營運持續管理系統 基礎課程	16	**4/15-16**、**6/3-4**、**8/12-13**、**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	**1/21-25**、**4/22-26**、**7/15-19**、**12/23-27** 假日班：**5/2-4, 10-11** 高雄班：**3/18-22**、**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	**3/11-12**、**3/11-12**	NT$ 22,000
	ISO 20000-1:2018 IT 服務管理系統 內部稽核員訓練課程	16	**2/21-22**、**8/22-23**	NT$ 20,000
	ISO 20000-1:2018 IT 服務管理系統 建置實務課程	24	**6/10-12**、**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	**2/18-22**、**5/20-24**、**8/5-9**、**11/4-8**	NT$ 55,000
	ISO 29100:2011(CNS 29100)隱私框架 國際標準基礎課程	8	**1/21**、**5/13**、**8/5**、**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	**1/21-22**、**4/8-9**、**6/3-4**、**8/5-6**、**10/7-8**、**12/16-17**	NT$ 15,000
	BS 10012:2009 個人資訊管理系統 國際標準基	8	**3/11**、**7/1**、**9/2**	NT$ 8,000

課程類別	課程主題	時數	預定開課時間	課程費用
	礎課程			
內稽系列	內部稽核實作基礎班**(**初任課程**)**	12	**3/11-12**、**11/11-12**	NT$ 6,600
	💻自行評估問卷設計標準範本_內控法規 COSO 五大組成要素	7	**1/29**、**8/29**	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	**3/19**、**11/26**	NT$ 3,850
	💻應用簡報視覺化技巧呈現經營管理與稽核報告	7	**6/25**、**11/25**	NT$ 3,850
	NEW!內部稽核有效應用財務報表實務班**(**初任課程**)**★	6	**1/21**、**10/21**	NT$ 3,300
	💻資料分析軟體應用技巧與查核實務	6	**3/7**	NT$ 3,300
	提昇「內部稽核價值」有效作法	6	**4/23**	NT$ 3,300
	NEW!內部控制研發循環與智慧財產權管理★	6	**5/16**	NT$ 3,300
	💻實作持續性稽核平台 - 以 ACL 與 Excel 為例	6	**5/31**	NT$ 3,300
	內部稽核協助提昇「組織價值」有效作法★	6	**6/3**	NT$ 3,300
	NEW!當 IA 遇到 AI★	6	**8/2**	NT$ 3,300
	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_查核六大循環作業	15	**1/18-19**、**6/18-19**、**10/23-24** **12/18-19**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_函數初中級課程**(**初任課程**)**	15	**2/26-27**、**7/24-25**	NT$ 7,500
	NEW!💻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	**3/26-27**、**9/9-10**、**12/26-27**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_資料處理初級課程	15	**4/25-26**、**9/24-25**	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	**5/28-29**、**11/28-29**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_樞紐分析進階課程	15	**6/26-27**、**10/15-16**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_企業採購查核作業	15	**8/22-23**	NT$ 7,500
	NEW!💻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	**1/22**、**3/22**、**5/22**、**7/22**、**10/22**、**12/23**	NT$ 3,850
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_圖表製作基礎課程**(**初任課程**)**	7	**2/23**、**7/23**	NT$ 3,850
	NEW!💻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	**2/25**、**4/29**、**7/29**、**10/29**	NT$ 3,850
	💻從 Big Data 樞紐分析查核 Power BI_擅用五大軟體繪製圖表	7	**4/30**、**8/30**	NT$ 3,850
	💻從 Big Data 關聯式資料查核 Power BI_透視視覺化圖表分析	7	**5/27**、**9/17**	NT$ 3,850
	💻提升電腦專業查核_匯總 Excel 屏棄不用函數避免當機	7	**5/21**、**8/21**、**11/21**	NT$ 3,850
	作業系統與通信傳輸查核★	6	**3/5**、**10/8**	NT$ 3,300
	電腦輔助稽核技術與工具(CAATTS)應用演練★	6	**3/28**	NT$ 3,300

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	網站安全與稽核簡介(Ⅰ)★	6	**4/12、8/12、11/6**	NT$ 3,300
	網站安全與稽核簡介(Ⅱ)★	6	**4/24、8/14、11/13**	NT$ 3,300
	數位時代電腦稽核起手式**(**初任課程**)**★	6	**4/22、9/2**	NT$ 3,300
	資訊部門稽核與資訊系統控制查核★	6	**5/9、11/7**	NT$ 3,300
	行動應用 APP 安全檢測與實務★	6	**5/10**	NT$ 3,300
	以數據分析解析營運流程與財務舞弊偵測★	6	**5/23、10/3**	NT$ 3,300
	網路安全風險評估與系統復原力管理★	6	**5/30**	NT$ 3,300
	雲端服務管理稽核★	6	**6/4**	NT$ 3,300
	資料存取於稽核與行為分析之應用	6	**6/13**	NT$ 3,300
	數位時代電腦稽核實務研習**(**初任課程**)**★	6	**6/17、10/7**	NT$ 3,300
	ERP 系統控制測試與稽核★	6	**6/20**	NT$ 3,300
	有效成本管控設計與分析★	6	**6/21、11/15**	NT$ 3,300
	稽核分析在銷售收款循環稽核個案演練(Arbutus 上機操作)	6	**6/28**	NT$ 3,300
	營運持續管理稽核實務 - 以稽核活動檢視組織韌性與復原力★	6	**7/4**	NT$ 3,300
	Excel 結合大數據分析(Ⅰ)：Power BI 資料擷取與多元資料分析	6	**7/11**	NT$ 3,300
	大數據環境下持續性稽核與風險評估最佳實務★	6	**7/12**	NT$ 3,300
	應用系統導入 PKI 安全機制與檢查	6	**7/15**	NT$ 3,300
	採購及銷售循環數據稽核 - 高風險交易資料分析	6	**7/26**	NT$ 3,300
	銷售收款與採購付款舞弊電腦查核技巧★	6	**7/30**	NT$ 3,300
	以提昇企業價值為核心之企業資訊治理架構 COBIT 5 理論與實務介紹★	6	**8/6**	NT$ 3,300
	Excel 結合大數據分析(Ⅱ)：Power BI 視覺化分析與風險評估	6	**8/7**	NT$ 3,300
	稽核分析在採購付款循環稽核個案演練(Arbutus 上機操作)	6	**8/16**	NT$ 3,300
	COBIT 5 框架下 ERP 應用系統控制與稽核實務★	6	**9/6**	NT$ 3,300
	新時代稽核變革及實務案例分享★	6	**9/23**	NT$ 3,300
	談資安事件應變機制及稽核重點★	6	**10/4**	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
	網路與系統安全實務查核★	6	**11/8**	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
舞弊稽核與數位鑑識系列	新興科技環境的數位鑑識挑戰與因應★	6	**1/25**	NT$ 3,300
	NEW!內部稽核舞弊偵查應用技巧實作班**(**初任課程**)**★	6	**2/18、11/18**	NT$ 3,300
	NEW!資安事件應變處理與數位鑑識整合實務	6	**2/22**	NT$ 3,300
	數位鑑識於機密資料外洩稽核應用實務★	6	**3/8**	NT$ 3,300

課程類別	課程主題	時數	預定開課時間	課程費用
舞弊稽核與數位鑑識系列	常見駭客入侵手法說明及滲透測試檢測實務★	6	**3/15**	NT$ 3,300
	NEW!舞弊風險防範與因應★	6	**3/18**	NT$ 3,300
	網路與系統日誌分析實務操作	6	**4/10**	NT$ 3,300
	以稽核角度認識數位鑑識運用實務★	6	**4/11**	NT$ 3,300
	反制賄賂與貪腐法遵控制與稽核技巧★	6	**5/3**	NT$ 3,300
	NEW!舞弊調查實務★	6	**5/17**	NT$ 3,300
	NEW!舞弊調查人員應認知的數位鑑識實務	6	**6/6**	NT$ 3,300
	NEW!💻利用數位鑑識分析人員不當行為	6	**7/18**	NT$ 3,300
	NEW!營業秘密法實務案例解析與證據攻防★	6	**7/31**	NT$ 3,300
	以數位鑑識原則執行事發現場數位證據保全實作★	6	**8/15**	NT$ 3,300
	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
	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
個資外洩與保護系列	資料庫稽核與個資保護★	6	**1/17**、**10/17**	NT$ 3,300
	個人資料保護建置★	6	**6/14**	NT$ 3,300
	歐盟 GDPR 合規與個人資料保護★	6	**7/9**	NT$ 3,300
	如何建構個資管理機制★	6	**8/8**	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	**3/8**、**6/14**、**9/20**、**12/13**	NT$ 8,000
	Fintech 的發展趨勢、風險控管與稽核因應★	6	**6/12**	NT$ 3,300
	Fintech 應用與相關科技風險★	6	**7/19**	NT$ 3,300
	PCI DSS 資料安全標準與電腦稽核實務★	6	**8/9**	NT$ 3,300

※ 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。

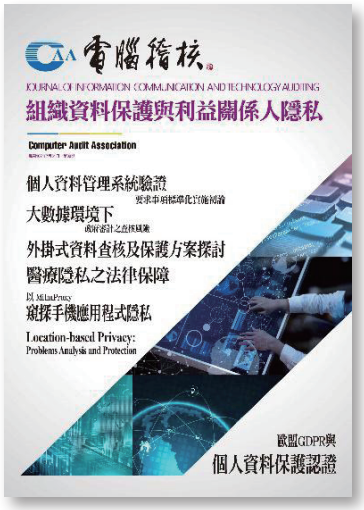
※ 可申報進修時數：實際可申報時數請依本會網站公告為準

- ■ 證期局公開發行公司內部稽核人員訓練時數
- ■ 證券期貨局內部稽核人員初任職前訓練時數
- ■ 證券期貨局內部稽核人員在職或替代訓練時數
- ■ 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
- ■ 銀行局信用卡業務內部稽核人員在職訓練時數
- ■ 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
- ■ 保險局保險業內部稽核人員在職訓練時數
- ■ 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
- ■ 投信投顧公會內部稽核人員訓練時數
- ■ 公務人員終身學習時數(限 ISACA 證照及 ISO 課程)
- ■ CISA、CISM、CGEIT、CRISC、CIA 學習時數
- ■ 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。

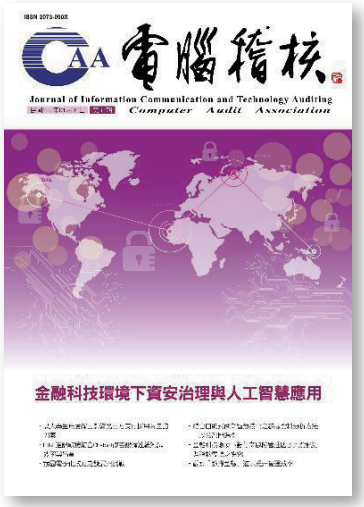
電腦稽核期刊前期篇名整理

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

第三十七期_金融科技環境下資安治理與人工智慧應用



- 以大學生角度探討影響第三方支付採用意圖的因素
- LINE 通訊軟體結合 Chatbot 改善設備連線測試效率與品質
- 我國電子化政府之發展與挑戰
- 結合自助式商業智慧技術之敏捷資料分析方法—以公部門為例
- 金融科技環境下銀行業風險管理因子與資訊治理稽核要項之探究
- 觀察「數據型態」進以提升營運效率

訂購詳見電腦稽核協會網站http://www.caa.org.tw/publish.asp

ISACA摘譯期刊近期篇名整理

第20期　　2018年06月出刊

- ◆ 二十一世紀中葉之資訊倫理
  Information Ethics in the Mid- 21st Century
- ◆ IT 查核人員所需的進階資料 (或數據) 分析
  Advanced Data Analytics for IT Auditors
- ◆ 以機器學習方法進行遠端醫療治理
  A Machine Learning Approach for Telemedicine Governance
- ◆ 使用開源工具協助科技治理
  Using Open Source Tools to Support Technology Governance
- ◆ 你需要災難復原計劃嗎 ・・・ ?
  Do You Need a Disaster Recovery Plan…?
- ◆ 如何將分析轉換為內部稽核
  How Analytics Will Transform Internal Audit

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

訂購詳見電腦稽核協會網站http://www.caa.org.tw/publish.asp

近期活動報導

2018.07.24

7 月台北例會

【 洗錢評鑑、導入風險與內控防制作為 】

匯豐銀行今年因高層涉嫌將部分收入存入瑞士銀行戶頭的方式逃漏稅，以及於 2012 年爆出為墨西哥、哥倫比亞地區不法集團提供帳戶的洗錢案。兆豐金控則因 2016 年風險管理及防制洗錢制度未達監理機關標準的缺失，遭美國裁罰，並於今年度受美國不同監理機關對於同一時期的缺失作處分。以上種種案例皆顯示出台灣銀行業內控不彰等種種問題。

◆ 7 月台北例會 - 臺灣高等法院檢察署 許永欽檢察官

本次例會活動邀請臺灣高等法院檢察署許永欽檢察官以洗錢評鑑、導入風險與內控防制作為主題，以實際案例分析台灣洗錢評鑑之問題及公司治理現狀，以法遵及法效為主體點出治理困境與問題，並分享如何以風險導向提高反洗錢內部稽核實務有效性，最後介紹防制洗錢之內控監管理架構及實務，結合理論及實務，期望能幫助學員了解及實際應用與工作中。

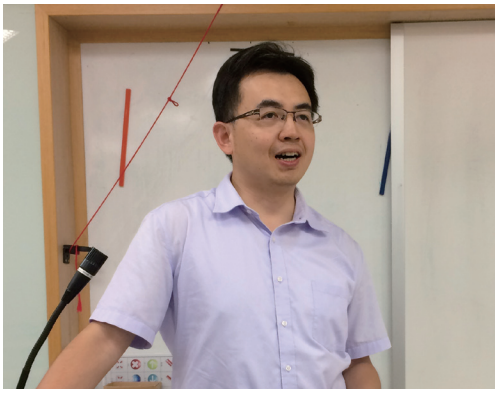
7 月新竹例會

2018.07.26

【 符合 GDPR 的資料保護衝擊評鑑 (DPIA)】

GDPR 歐盟一般資料保護規章正式於今年 5 月 25 日正式實施，實施初期部分企業認為經營項目或客戶非歐盟國家即不須重視此規章，直至今年下半年才發現基於整體供應鏈安全因素，也必須符合 GDPR 的規範。

本次例會活動邀請國立高雄科技大學金融資訊系魏銷志助理教授以符合 GDPR 的資料保護衝擊評鑑 (DPIA) 為主題，介紹 GDPR 對 DPIA 的要求、目的及程序，並以 ISO/IEC 29134: 2017 為執行方法，對 ISO/IEC 29134: 2017 進行深入淺出的解說，同時也詳盡介紹 PIA 的執行程序、報告架構、風險評估及公開摘要，提供學員在實務中執行 DPIA 的方法，使企業能有效符合 GDPR 的規範，避免不必要的花費與責罰。



◆ 7 月新竹例會 - 國立高雄科技大學金融資訊系魏銷志助理教授

協辦

2018.07.31

「2018 台灣企業舞弊風險調查報告 」研討會

科技大量應用於企業內輔助工作的進行，促使國際間的貿易蓬勃發展，行使便利工具的同時相關風險也隨之增加，國際間各種法令規範以及相關罰則更是不容小覷，企業除應重視內部潛在舞弊風險外，如何應用創新科技於治理層面將風險降至最低，已是如今更為重要的一環。

本次研討會為勤業眾信聯合會計師事務所主辦，本會協辦，首次發布《2018 台灣企業舞弊風險管理調查與未來展望》報告，邀請國內企業稽核、法務／法遵、財會、風管等領域人員參與問卷調查，收集並歸納 250 份有效問卷，總結各行業所面臨的風險類型及應對方法。本次活動邀請勤業眾信聯合會計師事務所賴冠仲總裁、金融監督管理委員會鄭貞茂副主任委員、國立交通大學科技法律研究所林志潔教授、勤業眾信銀行產業陳盈州負責人參與此次活動，分享企業舞弊風險的危害及因應策略。勤業眾信風險管理諮詢股份有限公司吳佳翰總經理分享從公司文化著手，強化舞弊風險管理，輔以資訊科技的應用進行數據分析以提早發現問題。勤業眾信風險管理諮詢股份有限公司曾韵執行副總經理分享零容忍的態度是防範弊病的重要方針，並建構良好偵測、揭弊環境，落實查核，以建立有效的管理環境。電腦稽核協會張紹斌理事長以自身經驗分享企業發生商業犯罪事件進行訴訟時，經常因為企業對於數位證據概念不足或缺少相關保全工具，導致未能及時保存證據或證據被汙染，企業應重視並妥善規劃團隊及運用工具，以取得合適、有效的數位證據。

◆（右起）勤業眾信風險管理諮詢股份有限公司吳佳翰總經理、勤業眾信風險管理諮詢股份有限公司曾韵執行副總經理、勤業眾信聯合會計師事務所賴冠仲總裁、金融監督管理委員會鄭貞茂副主任委員、中華民國電腦稽核協會張紹斌理事長、國立交通大學科技法律研究所林志潔教授、勤業眾信銀行產業負責人陳盈州先生

2018.09.01「從創新經濟看新時代的資安治理與稽核」專業論壇暨第 13 屆第 1 次會員 (代表) 大會及第 13 屆理監事選舉

在現今的數位時代中，面對變化迅速的科技應用，產業經營環境與經濟生態也隨之帶來重大變革，更是現今我國政策推動的主流。自 105 年底行政院發佈為期 8 年的「數位國家創新經濟發展方案」後，接續大數據應用的議題，期間在 106 年間金融科技、區塊鏈、人工智慧、機器學習等議題持續熱議，再加上甫於今年 5 月剛立法完成的資通安全管理法，及配套的產業發展方案，都可看到政府的重視程度。總統曾宣示「資安即國安」，資訊安全與治理能力在此創新經濟發展趨勢之下，應該做為最底層的基石，資訊與稽核人員也勢必要持續瞭解創新經濟相關的風險與因應之道。

此次會員大會以「從創新經濟看新時代的資安治理與稽核」為主軸，上午邀請國家通訊傳播委員會詹婷怡主任委員以數位時代的網路治理為主題進行分享。下午先以創新經濟與產業發展的現況與未來為主題，由行政院資通安全處簡宏偉處長分享資通安全管理法實施後的資安與稽核人材培育、經濟部資訊中心馬正維主任分享資通安全產業在創新經濟下的機會與挑戰。而後再以創新時代資安治理與稽核應有之思維為主題，邀請安永、安侯、勤業三大會計師事務所分享機器人流程自動化於風險三道防線的應用、面對 IoT/IIoT 的大航海時代，所面臨的安全衝擊以及從未來犯罪談 AI 人工智慧與企業資安治理任務等豐富精采內容。

◆ 第 13 屆第 1 次會員 (代表) 大會 - 左圖 (左起) 安永聯合會計師事務所傅文芳所長、國家通訊傳播委員會 (NCC) 詹婷怡主任委員、電腦稽核協會張紹斌理事長、勤業眾信聯合會計師事務所吳佳翰風險諮詢部營運長、中華民國內部稽核協會蕭家旗副理事長、安侯建業聯合會計師事務所張允洸執行副總經理；右圖安永聯合會計師事務所傅文芳所長與 ISACA 證照考試前三名得獎人合影

9 月台北例會

2018.09.25

【 企業如何面對新世代破壞式攻擊 】

隨科技的演進，攻擊工具的容易獲取性、多樣性，導致各種惡意攻擊屢見不顯，過去這兩年可見利用漏洞疏失竊取金錢、勒索，亦或是利用病毒感染破壞生產流程致使企業損失獲利等案件的大幅提升，一再提醒企業正視內部控制及安全防護的力度，隨時掌握最新攻擊趨勢並做出因應計畫更是首重之重。

◆ 9 月台北例會 - 安侯企業管理股份有限公司資訊科技顧問諮詢林大馗協理

此次月例會邀請安侯企業管理股份有限公司資訊科技顧問諮詢林大馗協理，以企業如何面對新世代破壞式攻擊為主題，帶領大家回顧這兩年發生的眾多針對型破壞式攻擊事件，再以常見攻擊為範例，從攻擊者的角度介紹、剖析攻擊思路，並以高科技廠商遭受的破壞式攻擊為例進行技術剖析，最後提出全面預防破壞式攻擊的 9 個方法，期望企業在安全防護上更為重視並做好萬全的準備。

2018.09.27

第十三屆第一次理監事會議 - 常務理監事、理事長選舉

第十三屆常務理監事、理事長選舉於電腦稽核協會舉行，投票結果為理事長由張紹斌律師續任，副理事長由蒲樹盛總經理擔任，常務理事由黃明達教授、張碩毅教授、莊盛祺總經理、孫嘉明教授、萬幼筠董事擔任。

◆ 第十三屆第一次理監事會議暨常務理監事、理事長改選

2018.09.27

9 月新竹例會

【 網路與系統及資料實務查核 】

近幾年臺灣遭受駭客攻擊事件頻傳，先有臺灣第一銀行 ATM 遭駭事件，而後又有遠東國際商業銀行遭植入木馬程式，入侵匯款系統 SWIFT 盜轉 18 億，分別轉入柬埔站、斯里蘭卡以及美國，且銷毀或加密帳戶資訊，導致追查困難。直至今年底美國網路安全公司才調查出近幾年 11 國家 16 間銀行遭駭皆為隸屬北韓駭客組織的 APT 38 所為。強化交易安全性，落實控管與稽核，提升員工警覺性，才有可能避免損失。

◆ 9 月新竹例會 - 欣盟科技有限公司技術服務部陳盛昌產品經理

此次月例會邀請欣盟科技有限公司技術服務部陳盛昌產品經理以網路與系統及資料實務查核為主題，分享近年台灣地區銀行遭受駭客入侵事件為例，強調風險評估的重要性，並以系統異動稽核、電腦漏洞稽核和資料稽核三方面入手，期待透過實務查核降低風險，為學員在實務上提供具體有效的執行方針。

9 月南區例會

2018.09.28

【 從遵循和實務角度談內控內稽 】

在臺灣，企業內部控制的制度從國 75 年草創，歷經 16 年達成法制化，而後又經歷種種修正與改革，直至今日仍在不斷變換的環境中尋求進步，可惜現實環境中仍有許多實務上的限制，如內稽受限、內控先天缺失、地位與角色如同東廠錦衣衛、支持與資源不足等等，仍需要稽核人員共同努力，以提升專業價值。

此次月例會邀請中華民國內部稽核協會高雄分會會長、華宏新技股份有限公司稽核室總稽核邱正德先生，從內部控制的歷史演進，分享法令與實務中的均衡，和專業價值與內部環境的衝突，在經營、法遵、財務、人資等不同面相中以創新求變的方式進行應對及溝通，並以自身實務經驗分享給學員，期望學員能夠自我肯定且具專業價值的優秀稽核人員。

◆ 9 月南區例會 - 中華民國內部稽核協會高雄分會會長、華宏新技股份有限公司稽核室總稽核邱正德先生

參訪交流

2018.10.15

北京市內部審計協會

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，由本會張紹斌理事長代表接待，並由黃秘書長簡報電腦稽核目前在台灣的發展與運用。

◆ 北京市內部審計協會參訪交流

2018.10.18 10月台北例會

【數位時代 E-Assurance 的關鍵成功要素】

金融監督管理委員會近年來持續推動風險導向內部稽核制度，增訂《金融控股公司及銀行內部控制及稽核制度實施辦法》第15-1條，銀行可向主管機關申請核准採行「風險導向內部稽核制度」，使相關產業的稽核角色更具獨立性、更能聚焦風險檢查以及稽核資源有效分配等等益處。

此次例會活動以數位時代 E-Assurance 的關鍵成功要素為主軸，邀請資誠聯合會計師事務所林維琪執業會計師以風險導向內部稽核制度與內部控制三道防線之有效運作為主題，分享世界先進各國及領導企業已採行之三道防線架構建置風險管理及內部監控系統框架，並介紹風險導向內部稽核制度之執行方式，以及內部稽核品質評核內容。

◆ 10月台北例會 - 兆益數位股份有限公司莊盛祺總經理

同時也邀請兆益數位股份有限公司莊盛祺總經理以企業資訊治理與持續性確認為主題，分享 COBIT 5 流程參考模型以及治理、風險管理、合規性和營運確保科技解決方案，以期達成良好的公司治理制度。

2018.11.23

11 月台北例會

「創新與變革：電腦稽核與資安治理的新契機」專業論壇

為推廣介紹 ISACA 系列證照及提供專業人士交流機會，此次專業論壇活動結合 ISACA 聯誼會，於台北凱撒飯店舉行。此次專業論壇以創新與變革：電腦稽核與資安治理的新契機為主軸，上半場邀請財團法人國家實驗研究院陳政龍正工程師以並肩電腦稽核專業人士一起洞悉國際電腦稽核的未來發展方向為主題，推廣 ISACA 的 4C 證照以及分享最新 COBIT 2019 發布消息；兆益數位股份有限公司莊盛祺總經理以 COBIT 5-- 對組織資訊系統的信賴及價值的創造為主題分享 COBIT 如何應用於企業內部控制及風險管理中。

◆ 11 月台北例會 － 左起安永企業管理諮詢服務股份有限公司周旺瑩經理、勤業眾信聯合會計師事務所風險諮詢服務陳鴻棋協理、電腦稽核協會張紹斌理事長、財團法人國家實驗研究院陳政龍正工程師、安侯企業管理股份有限公司資訊科技諮詢服務郭宇帆協理、兆益數位股份有限公司莊盛祺總經理

下半場以電腦稽核與資安治理實務議題分享為主軸，邀請勤業眾信聯合會計師事務所風險諮詢服務陳鴻棋協理、安侯企業管理股份有限公司資訊科技諮詢服務郭宇帆協理以及安永企業管理諮詢服務股份有限公司周旺瑩經理，分別以資安管理發展趨勢與展望、面對資安專責化的熱浪來襲，您該如何因應以及資料保護治理框架概述為主題，現場互動熱烈，為專業領域學員帶來稽核實務精采豐富的內容。

2018.11.29

11 月新竹例會

【異常行為分析與稽核】暨聯誼會

此次月例會活動結合一年一度新竹地區電腦稽核相關人士之聯誼會，邀請安永聯合會計師事務所企業管理諮詢服務黃誌緯資深經理，以異常行為分析與稽核為主題，分享今年度安永聯合會計師事務所進行的全球資訊安全調查報告結果，總結隨著組織數位轉型後所面臨的風險與威脅，探討企業在實務中所面臨異常行為對資訊保護的挑戰，並提出異常防護、稽核及第三方風險控管的方法與工具。

而後由安永聯合會計師事務所鑑識會計與法遵服務龍玉玲資深經理，以舞弊偵防與異常行為分析實務探討為主題，分享舞弊的種類及企業最常面臨的舞弊困境，提出企業內部控制及反舞弊計畫架構和因應策略，以實際案例運用數位鑑識分析進行異常行為分析及舞弊調查。最後全體學員共同交流互動並享用茶點，實為收穫良多的一場月例會暨聯誼會活動。

◆ 11 月新竹例會 - 安永聯合會計師事務所企業管理諮詢服務黃誌緯資深經理、安永聯合會計師事務所鑑識會計與法遵服務龍玉玲資深經理

12 月南區例會

2018.12.18

【 數位轉型與電腦稽核發展趨勢 】

科技發展使數位化力量造就數位經濟時代來臨，如大數據、人工智慧、雲端科技、區塊鏈等皆是造就數位轉型的重要原因，而這些因素帶來的利益背後同時也隱藏著眾多風險以及對社會的衝擊與挑戰，如 2030 年人工智慧取代大量單一、重複性工作，或是特斯拉自動駕駛遭駭客入侵、Facebook 侵害使用者隱私等。

本次例會邀請到國立雲林科技大學會計系孫嘉明副教授，以數位轉型與電腦稽核發展趨勢為主題，分享近年來數位轉型與產業數位化所帶來的影響，以及以實際案例分享數位轉型的機會與風險，並探討數位轉型對審計、內部稽核所帶來的影響，與電腦稽核的未來發展趨勢。最後介紹國際電腦稽核協會 (ISACA) 持續推廣的 4C 證照，期望學員關注國際趨勢，躍升國際優秀電腦稽核人士。

◆ 12 月南區例會 - 國立雲林科技大學會計系孫嘉明副教授

2018.12.20

第十三屆第二次理監事會議

108 年各委員會工作事項與財務預算審查及報告協會會址搬遷進度。

◆ 第十三屆第二次理監事會議

12 月台北例會

2018.12.27

【 強化 OT 資安防護策略 】

隨著網際網路與 IT 普及，OT 與 IT 的環境隔閡日漸消失，且全球針對性攻擊的資安事件日益增多，如 2010 年伊朗核能設施工控系統的駭客攻擊、2014 年德國鋼鐵廠資安事件、2015 年烏克蘭電廠資安事件等，探討事件軌跡後發現其攻擊概念基本上都十分相似，儘管安裝防毒程式，監控機制仍不可缺少。

本次例會邀請到勤業眾信聯合會計師事務所企業風險服務陳威棋協理以強化 OT 資安防護策略為主題，分享全球近年來所面臨的資安事件、風險及趨勢，並以各國實務案例分析攻擊概念及模式，而在資安事件不可全然避免下其因應對策為何，以及分享國際資安最佳的工業自動化及控制系統實務，讓學員能將此次分享內容帶回公司改善 OT 資訊安全環境。

◆ 12 月台北例會 - 勤業眾信聯合會計師事務所企業風險服務陳威棋協理

ISACA®

Trust in, and value from, information systems

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**

CISA Certified Information Systems Auditor®
An ISACA® Certification
國際電腦稽核師

CISM Certified Information Security Manager®
An ISACA® Certification
國際資訊安全經理人

CGEIT Certified in the Governance of Enterprise IT®
An ISACA® Certification
國際企業資訊治理師

CRISC Certified in Risk and Information Systems Control™
An ISACA® Certification
國際資訊風險控制師

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。

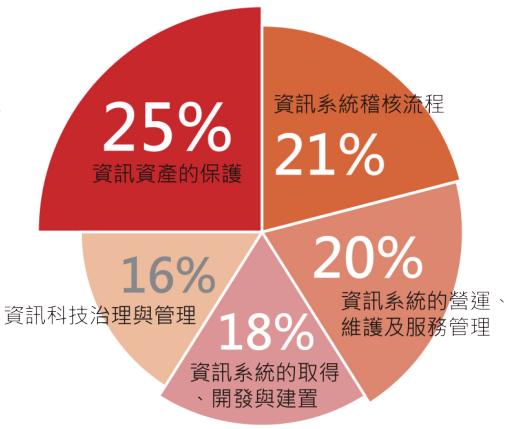
國際電腦稽核師證照(Certified Information Systems Auditor® , CISA®)是毋庸質疑的認證，當您擁有CISA證照，您的專業將立即得到理解與認同，CISA證照將讓您在國內與國際上對於使用標準、確認管理缺失、法規符合性，提供解決方案、發展控制措施以提供企業價值的專業知識、技能、經驗與可信賴的認可。

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。

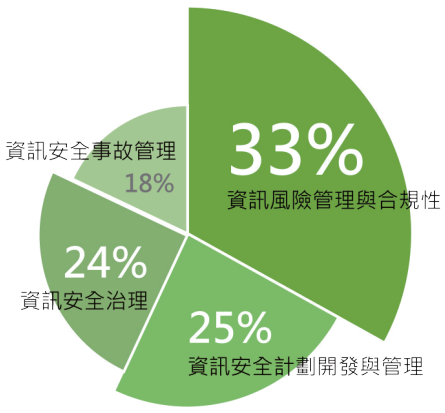
取得CISM的專業人士瞭解企業的需求，他們知道如何去管理和適應他們企業與行業的安全需求。CISM將不僅是具備資訊安全的專業知識，同時也在資訊安全的系統開發與管理上具有可靠的經驗。

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。

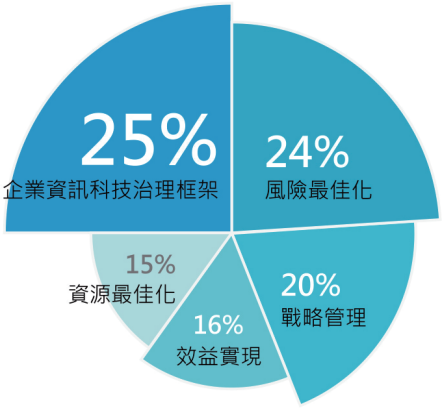
國際企業資訊治理師(Certified in the Governance of Enterprise IT® ,CGEIT®)認可的專業人士具備對於企業資訊治理的原則與實踐有廣泛的知識與經驗。作為一位CGEIT的專業人士，您將證明您具有在一個組織中資訊治理的能力，由整體面掌握複雜的議題，並因此而提升對企業的價值。

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。

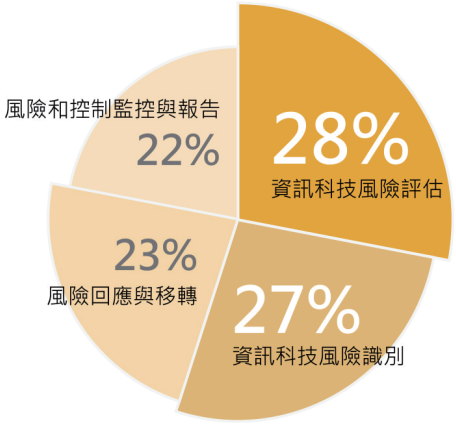
CRISC是最新且經過嚴格評核，具備識別資訊技術風險與評估資訊業務與風險管理的專業人士。CRISC證照將使您在企業內部資訊運作的未來發展上，提供更好的諮詢機會，並且使您在組織中的角色更顯重要；資訊風險將成為企業整體風險重要的組成部分，並使您在組織的資訊風險議題上成為知識型的領導者與內部規則變更的推動者。

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



ISACA

ISACA CERTIFIED, MEANS QUALIFIED.

www.isaca.org/GetCertified-Jv1

CISA國際電腦稽核師認證研習班
假日班：3/9、3/16、3/23、
3/30、4/13(六)
平日班：4/15(一)~4/19(五)

CISM國際資訊安全經理人認證研習班
假日班：4/20、4/27、5/4 (六)

CISA CRISC CISM CGEIT

日期	期程1 2/1~5/24
報名截止日期	5/18
延期截止日期	5/23

※費用：ISACA 會員：US $575
非ISACA會員：US $760

Call for Papers
電腦稽核期刊
全年度徵稿邀約

電腦稽核期刊參與 2017 年「臺灣人文及社會科學期刊評比暨核心期刊收錄」評比，正式（首次）被「臺灣人文及社會科學引文索引資料庫」登錄為第三級期刊。

本期刊係中華民國電腦稽核協會為推動電腦稽核領域學術及實務發展，半年為一期出版電腦稽核期刊，任何與電腦稽核相關之學術論述或個案研究，未刊登於其他期刊者皆可投稿，敬邀各位會員與相關領域之先進們共襄盛舉，不吝將研究結果、工作上之心得或經驗投稿於本期刊，共同支持電腦稽核產業發展。

徵稿文章依論文內容分為二大主題：

- **專業論壇：**

  強調理論及實務並重，一方面暢談電腦稽核各個面相，另一方面則從實務面檢視電腦稽核在政府部門、私人企業乃至於學術單位的建置與落實情形。

- **新知園地：**

  著重將電腦稽核經驗分享、最新訊息或發展介紹給全體會員及相關大眾知曉。

**** 徵稿簡約 ****

- 投稿文章請以中文或英文撰寫，文稿請用 MS Word 處理，表格請另提供一份可編輯檔案，圖片請另附原始檔 (像素 300dpi)。
- 來稿請寄電子檔至 member@caa.org.tw，主旨請標註：「投稿電腦稽核期刊 _ 篇名」，與投稿類別 (專業論壇或新知園地)。
- 投稿文章評審程序依本刊審查之原則辦理。
- 專業論壇包括封面頁，摘要頁，正文，參考文獻及附錄（文稿格式請參閱本會官網最新消息「邀稿通知之附件 - 投稿規範與標準」），並請依順序編入頁碼。作者姓名及相關資訊僅能出現於首頁
- 新知園地請依順序編入頁碼，作者姓名及相關資訊僅能出現於首頁。

CAA 電腦稽核

11070台北市信義區基隆路一段143號2樓之2

2F.-2, 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

中華民國電腦稽核協會

第39期期刊

民國108年01月31日發行