電腦稽核
Computer Audit Association 民國110年08月31日 第44期
ISACA Taiwan Chapter

Challenges and Innovations of Computer Auding in Cross-border Epidemic Prevention

跨界防疫在電腦稽核之挑戰與創新

地圖會說話－商業管理及政府審計之應用

論人工智慧及電子監控之研究－以美國勞工法為例

行動App 安全風險評估與防範措施之研究

應用COBIT 2019制定企業治理策略

透過COBIT 2019框架指引達成企業的數位轉型

School Accounting Education in Japan －In Relation to Economic Development of the Country

編 輯 序

近年來全球環境快速變遷，不論是大自然或是人類社會環境，都在不可預期的變遷下發生重大災難和面臨生存危機。新型冠狀病毒肺炎疫情（COVID- 19）便是一起由病毒所引起的重大疾病案例。COVID- 19 疫情已經進入「全球大流行」的階段。思考如何防止國際疫情擴散、維護國人健康安全、建置完善的疫情風險管理機制與措施，從而降低對國家、社會、民生、經濟、與生存環境所造成的衝擊，是世界各國政府極度重視的首要工作。

世界衛生組織（WHO）呼籲，各國政府應對重大傳染病應做好關鍵準備，並對可能風險提供可回應的措施，如：（1）減緩並停止傳播，防止爆發和延遲傳播；（2）為所有病患，尤其是重症患者提供最佳護理；（3）減少流行病對衛生系統、社會和經濟活動的衝擊。國與國之間商務交流互動不斷，疫情事件更在雙邊區域往來頻繁的情形下，讓疫病境外移入為我國防疫工作帶來沉重壓力。跨界防疫之風險管理已成為國家防疫的施政重點項目。思考如何透過科技跨界創新來進行超前部署，為跨界防疫工作採取適當的政策與態度，並建立智能化電腦稽核與風險治理模式，為疫情找出創新的解決方案，是提升我國對疫情應變、整備和回應能力的關鍵挑戰。智能化跨界科技防疫治理，已儼然成為電腦稽核領域的新興應用，也是未來產業發展的新契機。思考如何透過物聯網設施提供零接觸式的防疫設備、發展智能化科技防疫稽核與控制，為疫情提供完善的疫病即時資訊、預警、與潛在風險之監控，是全球當前的熱門議題。

綜上所述，電腦稽核期刊第四十四期以「跨界防疫在電腦稽核之挑戰與創新」議題為主軸，邀請國內外學者與專家，提出具創新性與實用性論文，討論數位經濟環境下新興科技所帶來的機會與挑戰，以及思考如何運用電腦稽核技術讓疫病風險獲得有效的控制。本期收錄文章強調理論及實務並重，包括「地圖會說話 - 商業管理及政府審計之應用」、「論人工智慧及電子監控之研究 - 以美國勞工法為例」、「行動 App 安全風險評估與防範措施之研究」，一方面暢談新興科技應用的各個面向，另一方面，則從學術與實務面評述跨界防疫在電腦稽核與智慧治理的挑戰與創新，並提出可因應與解決的方法。新知分享方面則有「應用 COBIT 2019 制定企業治理策略」、「透過 COBIT 2019 框架指引達成企業的數位轉型」、「School Accounting Education in Japan—In Relation to Economic Development of the Country」著重數位環境下跨界科技防疫創新之應用與風險管理的新知與訊息，並將最新發展趨勢介紹給全體會員及社會大眾知曉。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秘書處之協助、各位審稿委員的細心審閱。本期期刊若有不盡之處，敬請各位先進賜教。

張碩毅

國立中正大學 管理學院院長

編譯出版委員會主任委員

電腦稽核
Challenges and Innovations of Computer Auding in Cross-border Epidemic Prevention
第 44 期

目　錄
CONTENTS

發 行 人：葉奇鑫
總 編 輯：張碩毅
編輯委員：温大民、李興漢、孫嘉明、徐立群、黃劭彥、張益誠、劉其昌、邵之美、諶家蘭
執行編輯：游恬欣
封面提字：林志雄
秘 書 長：黃涼澤
秘　　書：何慈雯、許秀玲

出版單位：中華民國電腦稽核協會
展 售 處：中華民國電腦稽核協會
地　　址：11070 臺北市基隆路一段 143 號 7 樓之 4
電　　話：(02)2528-8875
網　　址：https://www.caa.org.tw

視覺設計：品晟股份有限公司
印　　刷：品晟股份有限公司

發行日期：110 年 8 月 31 日
定　　價：新臺幣 250 元

地圖會說話
-商業管理及政府審計之應用

黃劭彥
國立中正大學會計與資訊科技學系教授
陳俊志
國立中正大學會計與資訊科技學系研究所博士生
高懿柏
審計部桃園市審計處薦任審計

摘　要

地理資訊系統在最近的 40 多年內以驚人的速度發展，廣泛應用於資源調查、環境評估、災害預測、國土管理、都市規劃、郵電通訊、交通運輸、軍事公安、水利電力、公共設施管理、農林牧業、統計、商業金融等各領域。本文期透過 GIS 構成的空間資訊技術，探討地理資訊系統如何協助企業應用及政府審計上作出更有效益之決策分析。

關鍵詞：地理資訊系統、政府審計、決策分析

Abstract

Geographic information systems(GIS) has developed an alarming speed in the past 40 years and been widely used in resource survey, environmental assessment, disaster prediction, land management, urban planning, post and telecommunication, transportation, military public security, water conservancy and electricity, public facility management, agriculture and forestry animal husbandry, statistics, commercial finance and other fields. This article uses the spatial information technology formed by GIS to explore how GIS can

assist enterprises in making more effective decision-making analysis in application and government auditing.

Keywords：GIS、Government auditing、Decision-making analysis

壹、地理資訊系統基本概念

地圖係人類描述地表空間事物之指引，製圖技術亦隨著現代文明科技的演化，結合地理資訊、電腦與電子科技的新興學科 —地理資訊系統（Geographic information system，簡稱 GIS）。

GIS 顧名思義乃是一種地理資料庫管理系統，是由「地理」、「資訊」、「系統」三者結合而成，凡與相對位置或空間分布有關的知識均屬於地理的範疇；GIS 係將電腦硬體、軟體、空間資料與使用人員相連結，組成一個系統，其最強大之功能可整合如交通、人文、灌溉系統、土地利用、土壤、雨量、地質、地形及水資源等各種具有空間分布特性之資料，各類電子圖籍經由 GIS 的套疊[1]、編修及分析後，可供資源規劃、生態保育、區位勘選等參考使用，進而提供更準確之評估及決策分析。

GIS 系統是近年來發展極為迅速的跨領域新科技，GIS 系統所涵蓋的理論和技術是由地理學、地圖學、測量學、統計學、數學、資訊管理 …… 等幾個基礎學科所發展，至於運用 GIS 系統所涵蓋的領域則更加廣闊，如環境工程、田野調查、國土規劃、都市計畫、交通管理、森林經營、運輸通訊、生態保育、考古調查 …… 等等，舉凡需要涉及地理技術或空間規劃的領域，皆可以利用 GIS 系統分析作為輔助。

GIS 系統能有效率地擷取、儲存、分析及展演各種形態的地理資訊，主要的系統組成包括軟硬體[2]、地理資料庫及專業技術人員，就 GIS 的運作而言，需要高投資的大規模電腦作業系統，通常系統的設置須由中央及地方政府或是企業投資建設，其主要目的是提供專業領域能有效率地管理利用資源，因為 GIS 可以透過疊圖及空間分析功能，迅速分析具有地理區位特性事物及現象，因此能將原始地理資料轉換為支援空間決策的資訊。

另外，對於 GIS 系統運作最關鍵的問題就是數位資料庫的建立，因其直接影響了資料儲存之效率，也間接影響了後續資料處理及分析之效能。簡言之，數位資料庫系統是 GIS 的中樞神經，主要功能是將地理資訊以數位方式妥善地儲存，並提供適當的資訊與使用者，一套完整的地理資訊系統，可以儲存廣闊的空間資訊，不但能迅速呈現出相關地區的電子地圖，更能符合需求，提供各種空間資訊，讓使用者在電腦螢幕上操作、疊合、重組、抽離，使其對自己的生活環境或週遭世界可以一目了然，迅速掌握，結合

1. GIS 圖層套疊：針對同一個面圖層，將同一欄位中相同值的圖徵合併。
2. ArcGIS Server 與 Arc SDE，ArcGIS Server 是建立 WEB GIS 平台的基礎軟體、Arc SDE 則是資料庫中介軟體，為建立 WEB GIS 平台基礎時不可或缺的重要模組。

地圖處理、數位資料庫與空間分析三項功能，正是地理資訊系統的最大特色。

地理資訊系統（GIS）之資料可概分為兩個部分，空間資料[3]（Spatial data）與屬性資料[4]（Attribute data）。所謂空間即指其地理區位（Geography location），地理空間上的相對位置，藉由點、線、面地形變化來描述地表和地球本身的形狀、位置，並建立彼此間位相關係[5]（Topology）來記錄各物件的空間位置與相對位置關係，通常都以地圖的方式來表示；屬性資料則是指描述性的資料，描述空間的特徵，由編號、區位、名稱、類型、尺寸等文字或數字所構成。

貳、地理資訊系統之基礎應用

目前專家學者把 GIS 基礎應用情形說明如下：

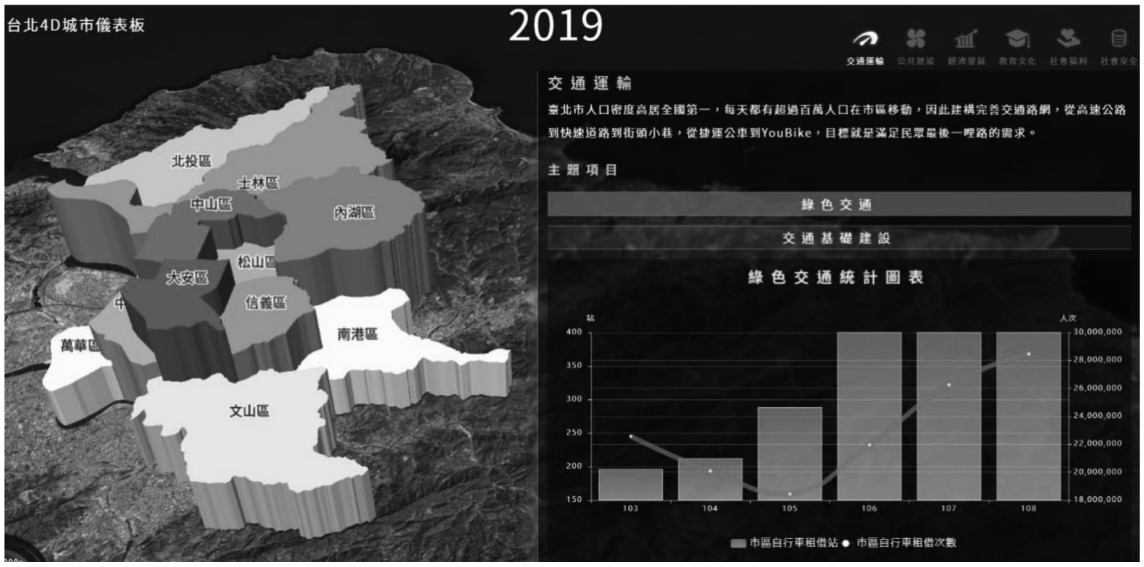
一、不同來源之模式分析

GIS 系統能就不同主題之空間與屬性資料進行分析，並將不同來源的資訊以不同的形式應用，例如：所在地的降雨與所在區域資料結合，判斷出哪塊濕地在一年的某些時候會乾涸。過去經典案例係 19 世紀英國倫敦之「霍亂傳播模式」研究，雖當時並無電腦化之 GIS 系統，惟 John Snow 醫生將霍亂之死亡案例繪製於倫敦的街道圖，且同時標示出抽水機之位置，並輔以相關統計研究分析，以提出霍亂係由飲水傳播之假設。又 GIS 同時也能將不是地圖形式的數字資訊轉換可辨識利用的形式，例如，通過分析遙感生成的數字衛星圖像，產製與地圖類似的有關植被覆蓋的數字資訊層。另外，政府機構與非政府組織透過 GIS 軟體，可將地圖中不同類型的資料格式比較分析，例如：人口調查或水文表格資料也可在 GIS 系統中被轉換成作為主題資訊層的地圖形式。

二、趨勢分析

運用長期蒐集之統計資料結合地理區域，進行趨勢分析。例如：臺北市政府建立的臺北 4D 城市儀表板，及新北市政府之城市儀表板，均係由 GIS 系統提供的行政區圖資，結合交通運輸、公共建設、經濟發展、教育文化、社會福利及社會安全等統計數據，以視覺化呈現人口消長與分布如下圖。

3. 空間資料為地理實體在空間分布的資料，例如山嶽、河川、道路和植物等在空間分布的位置、形狀、大小、結構等。
4. 屬性資料係描述地理屬性的資料，例如地名、土地疆界、道路寬度、土地利用類型等資料均屬之。
5. 位相關係係紀錄點、線、面資料之間的空間關係之表示，可由 GIS 自動產生。



資料來源：臺北 4D 城市儀表板 https:// 4d. taipei/

三、路線規劃

GIS 之應用不僅於道路之導航，在國外，消防隊可利用 GIS 系統，標示火警發生位置，消防車可行走，設計救火路線之案例，指示消防車可行走之最短路徑，並給予消防員火災所在之建築物平面圖、附近之消防栓、水線之布防，後續還可進行火災地點之頻率分析，以規劃最佳救火路線等決策。另外，GIS 系統在路線地規劃上，國外實務也有以大醫院做主要目標，再利用捷運的便利性作整合，以提供民眾獲得最佳就醫路線，並為了減少大人看診，小孩受感染的風險性，在距離捷運五百公尺內有醫院的位置，設置暫時托育所，使大人能放心就醫，小孩也能有完善的照顧，因而減少交叉感染的風險，並降低民眾的不安。

參、地理資訊系統之應用及限制

一、商業實務之應用

商業管理應用方面，隨著空間相關科技的推波助瀾，GIS 在國內外商業的應用也蓬勃發展，由於臺灣 GIS 系統的發展起步較晚，且受限於數位化資料與空間整合的問題，現今仍尚未完全普及，目前較為大眾所知的 GIS 系統應用，應為網路上各大搜尋引擎上的電子地圖，惟企業已逐漸地認知到，當電子地圖與各種行動商務結合，它將具有搖身一變，成為「火力強大的管理工具」的能力。

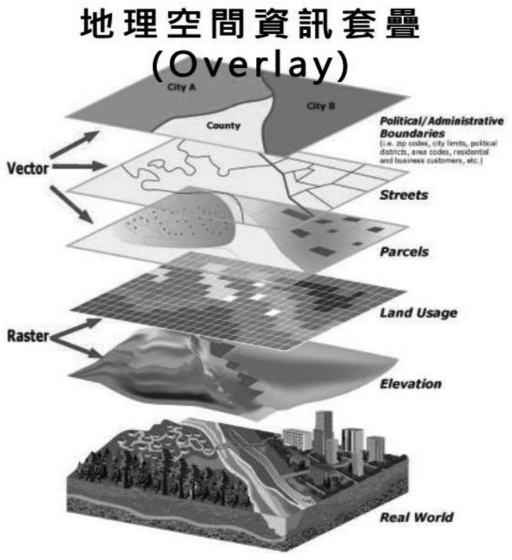
現已有部分零售業結合 GIS 工具來進行商業分析，以 GIS 為核心的空間資訊技術，將企業財務系統、銷售系統、工作流管理系統、客戶關係管理系統等融合，成為企業資訊化的業務平台。藉由 GIS 的資料庫建檔與查詢分析等功能，實現遠端及分散式計算，達到企業即時生產、零庫存、售後服務等有效管理。

另外，已有不少之金融業採用 GIS 工具做內部管理，將其作為內部擔保品作業管理的地圖工具。例如：臺灣銀行在 2013 年底就正式上線一個結合地理、空間資訊系統和內部管理數據的電子地圖作業平臺。平臺上

運用了空間資訊系統，整合公司內部作業原有的文字、數據資料，全面改用地圖方式來呈現。

過去銀行在處理如土地、建物等貸款擔保品申請案時，通常僅依承辦人員提供表格清單來稽核，只有在案件抽查才會親自到場勘估，因而在稽核品質得承擔一定風險。但透過整合 GIS 系統和公司內部管理數據，現在銀行總公司在稽核擔保品案件時，能在電子地圖上直接分析擔保品所在位置的周邊環境資訊，包括確認是否存在嫌惡設施或搜尋鄰近擔保品的過往記錄，比起過去僅靠表格清單呈現擔保品資料，更能掌握實際狀況，不僅提升稽核品質也降低擔保品抵押風險。

結合擔保品電子地圖平臺，金融業能直接在地圖上查詢擔保品案件範圍的周邊環境資訊，包括過去評估記錄，生活設施和嫌惡設施等提供更多資料佐證。而透過地圖上的篩選機制，也能利用擔保品案件的屬性分類，例如建築型態、建坪單價來呈現地圖結果，快速過濾出符合條件的案件。



資料來源：https://libguides.coloradomesa.edu/c.php?g=6138

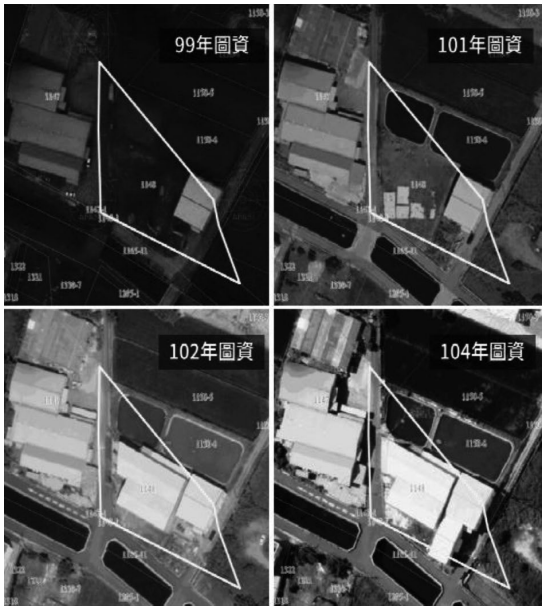
而除了作為金融企業擔保品的風險控管，透過 GIS 系統，承辦人員在撰寫擔保品評估報告時，也能直接使用 GIS 工具在電子地圖上繪製和操作，除了免除過往的人工繪圖方式，也縮短作業流程時間，甚至標示在地圖的擔保品案件，也能提供進階分析或從中找到更多附加價值。

另外，國泰人壽也整合 GIS 系統運用在公司內部的作業管理平臺，陸續也有多家金融企業，包括玉山銀行、第一銀行以及永豐銀行等，先後導入 GIS 成為公司內部運作管理的標準流程。

至於其他的應用方面，如觀光旅遊規劃方面，旅遊業或相關之產業亦皆可透過 GIS 系統作地點分佈、動線規劃。由上述例子可以得知，只要需要使用地圖的地方，即可使用GIS系統作為企業管理與風險控制之工具。

二、政府稽核實務運用

現行政府審計工作除以合規性、預算執行率、經費科目適切性及專案角度等考核政



資料來源：作者自行整理繪製。

府機關外，亦可透過空間面向考核政府機關之績效，例如：諸多閒置場館之產生，係因於公共建設投資未放在對的地方，亦或是有過度集中及分散之情形，主要問題出於空間配置，經由 GIS 之運用，可確認核定公共建設前及興建後之效益，是否進行完善地評估與後續的追蹤考核。

另外與土地使用相關之稽核議題，經由 GIS 圖層套疊即可進行外部整體性之稽核，例如：各地方政府公有房地清查管理情形 (套疊公有土地清冊，行政院農業委員會農地資源疑似工廠圖資及地理區域地籍圖資[6])、豪華農舍 (利用正射影像與非都市使用分區圖套疊)、國有土地之侵占 (利用正射影像與國有土地地籍圖套疊)，及國有非公用農地 (地籍套疊航照圖)、警察有無積極取締告發民眾舉發案件等問題。再者，如有相關規定係以距離或面積為基礎，例如：公告地價、大眾運輸事業補貼、電子遊戲場營業場所須距離學校一定距離或範圍等，均可利用 GIS 測量距離與面積，免除實際測量上困難。

三、限制

地理資訊系統擅長處理空間資料，但對於路網與時空問題仍有許多限制尚待克服。常見的 GIS 空間分析方法有時須判斷兩個位置的鄰近關係，如果未考慮路網之位相關係，演算法可能會將相鄰但不相接的兩個點誤判為有鄰近關係。

而空間分析的另外一個問題，經常未考慮路網的侷限性，導致結果無法忠實反映地表之真實情況。

肆、結論與建議

一、結論

大數據（Big Data）有許多可空間化的數據，像是座標、路線、範圍。這些就是空間大數據。經由 GIS 軟體，可加以分析並擷取出相關訊息。地理資訊系統這個軟體可以結合地理學與地圖學，廣泛的應用在不同的領域，以星巴克為例子，經由分析人口、商場位置、交通動線做為開店的依據，運用空間分析可以做出更有效益的決策。

隨著科技的日新月異，GIS 系統未來的應用範圍勢必逐漸擴大，當 GIS 所涉及的產業及領域越來越多元時，系統的整合性要求想必愈發緊迫，因此軟體的功能，是否足夠應付不同領域的需求，便為 GIS 未來發展相當重要之關鍵。而近年來各級政府部門對地理資訊之投入，使得 GIS 發展所需之各項圖資已達到一定的水準，相對較容易取得。

目前臺灣對於 GIS 的應用主要多用於地圖製作、資訊管理、以及與地理相關資料的登記管理，至於針對社會環境的探討與分析、決策的支援，目前的應用上仍相當有限，因此該如何持續整合資料與應用層級的多樣化，是現今 GIS 系統發展面臨的最大課題。

二、建議

空間資訊之技術產業應從政府與學界，擴散應用到產業界與相關 NGO 團體之跨領域應用及合作。

(一) 政府機關及企業得舉辦相關 GIS

6. 地籍圖資網路便民服務系統，https://easymap.land.moi.gov.tw/Home

之駭客松[7]（ hackathon）及工作坊，透過競賽及獎勵機制去促成更多資訊及地理相關人才投入，以提升空間資訊之技術產業能見度。

（二）現行我國空間資訊應用企業規模多屬中小型企業，且多為各自發展，自行研發成本龐大，政府得提供適當之經費補助與獎勵，或協助各中小企業平行整合與合作，創造資料加值應用。

（三）空間資訊產業應與新興科技 (大數據、物聯網[8]、AI、行動化應用、雲端應用) 等跨領域結合為必要之發展趨勢。

參考資料

1. 許忠義，2009，日本統計空間資訊技術之發展與應用。
2. 李文堯、林心雅，2007，地圖會說話 - 不可思議的 GIS，時報文化。
3. 周天穎，2008，地理資訊系統理論與實務。
4. 廖炫銘，2016，地理資訊系統與技術應用於審計工作，政府審計季刊 36(2)。
5. 周天穎，2018，我國空間資訊產業發展潛力與未來，國土及公共治理季刊 7(2)。
6. 曾彬凱、洪鳳儀，2015，地理資訊系統在政府審計之創新應用，國土及公共治理季刊 3(4)。
7. 張國楨，蔡詠名，2019，GIS 資料探勘與交通資料應用，國土及公共治理季刊 7(2)。
8. 陳志良，2013，淺談地理資訊系統基本概念與應用，主計月刊 691。
9. 施保旭，2000，地理資訊系統。臺北市：儒林。
10. 王明志、曾正雄、陳冠廷，2009，地理空間資訊製圖與建模研究，中華民國地圖學會會刊，19，97- 116。
11. 王怡驊，2019，地理資訊系統應用於縱火犯罪案件分析之研究 - 以臺中市為例，國立中興大學環境工程學系碩士論文。
12. 王遠飛、何洪林，2007，空間數據分析方法，科學出版社。
13. 洪美秀，2013，臺灣農地重金屬高污染潛勢區域篩選方法之探討，國立臺灣大學生物環境系統工程學系碩士論文。
14. 張嘉茹、杜鴻運，2019，肺結核在台灣中部地區的傳播與地理位置及環境因子間的關係 」，感染控制雜誌 29，81- 87。
15. 陳勝義，2008，台中市搶奪犯罪熱點與犯罪區位分析之研究，逢甲大學土地管理學系碩士論文。

7. 程式設計馬拉松（hackathon，又譯為駭客松），又稱程式設計節（codefest），是一個流傳於駭客（hacker）當中之新詞彙。
8. 物聯網（Internet of Things，IoT）是一種計算設備、機械、數位機器相互關聯的系統，具備通用唯一辨識碼（UID），並具有通過網路傳輸數據的能力，無需人與人、或是人與設備的互動。

論人工智慧及電子監控之研究

-以美國勞工法為例

On the Study of AI, Electronic Surveillance

-Take U.S.A. Labor Law as an Example.

許淑媛Cadalina Hsu
大洋法律事務所執行長
國立臺灣大學法學士及碩士
中正法博士候選人
C.E.O. at Da-Young attorney-at-law firm
B.A.&M.A at NTU, P.H.D. Candidate at CCU.
hsucadalina@gmail.com

摘　要

雇主和其他僱用員工來執行相關工作上之活動，並且讓員工使用許多電子機制，其中有關招聘、員工評估、薪酬、紀律等和保留這些電子機制，例如包括電子追蹤器、監控攝影頭、身體的代謝監測儀、測量裝置和其中的技術，雇主利用這些工具啟用來記錄他們員工的一切活動、聆聽他們的對話、測量績效的時間等方面，並檢測反對組織活動，收集通過的數據等等。因人工智慧演算法方法進入永久保存，電子簡歷也可以識別和預測人的績效以及他們的職業道德、個性、工會傾向、雇主忠誠度和未來醫療保健成本、電子簡歷等等。

由人工智慧生產的各種機制追隨員工從一項工作場所到另一項工作環境，因為他們移動圍繞網路世界無遠弗屆的工作場所，因此人工智慧和電子監控產生一個無

形的電子網路，不但入侵員工隱私權，還阻止工會運行，使微妙的雇主形式化加劇就業歧視問題，讓工會變成無法正常運作以及無法賦予勞工相關勞工法之保障。

本文介紹人工智慧在工作場所之運用及其使用如何改變招聘之實踐、評估、補償、控制和解僱員工。然後，專注於人工智慧威脅要破壞員工法律領域之保障 : 反歧視法、隱私權法、反托拉斯法和勞工法，最後，本文希冀能夠提出建議，為法律上未來提供相關改革和研究之方向。

關鍵詞：人工智慧、電子監控、電子網路、員工隱私權

Abstract

Employers and others who hire or engage workers to perform services use a dizzying array of electronic mechanisms to make personnel decisions about hiring, employee evaluation, compensation, discipline, and retention. These electronic mechanisms include electronic trackers, surveillance cameras, metabolism monitors, wearable biological measuring devices, and implantable technology. These tools enable employers to record their workers' every movement, listen to their words, measure the minutes of performance evaluation, and detect oppositional organizing activities.

The data collected is transformed by means of artificial intelligence (AI) algorithms into a permanent electronic resume that can identify and predict an individual's performance as well as their professional ethics, personality, union proclivity, employer loyalty, and future health care costs. The electronic resume produced by AI will accompany workers from job to job as they surround the boundless workplace in the cyber space. Thus, AI and electronic monitoring produce an invisible internetthat invade worker privacy as well as deter unionization, enabling subtle forms of employer blackballing, exacerbating employment discrimination. With these demerits, unions become ineffective and obliterate the protections of the labor laws.

This article describes the many ways AI is being used in the workplace and how its use is transforming the practices of hiring, evaluating, compensating, controlling, and dismissing workers. It then focuses on four fields of law in which AI threatens to undermine worker protections：Anti-discrimination law, privacy law, antitrust law and labor law. Finally, this article maps out an agenda for future law reform and research.

Keywords：AI, Electronic surveillance, Internet, Worker privacy

壹、前言

現今的工作場所已是無遠弗屆，但因此而發生的法律問題並沒有變得隨機即可處理，如今員工與支付服務費用的人有著許多不同類型的關係，這種關係從傳統的長期就業到短期隨機的兼職專案，當今的員工往往同時擁有多個雇主，這樣員工可以同時被大公司、特許經營商、臨時代理和現場承包商「受雇員」，因此員工也在許多不同的地點提供服務，包括他們的住宅、咖啡店、私人汽車、工作等等的共用空間，以及傳統的辦公大樓或工廠車間，此外，員工往往有多雇主或其他「參與者」加入也稱之員工。

雖工作場所位置可以隨時異動，然工作的流動性和雇主的身份難以捉摸，且員工在無形的電子網路中工作，該網路可以測量、量化、分析並刻劃出其工作經驗的基本象徵，而「無邊界工作場所」是員工與雇主之間的長期信任關係日益減弱，員工之間更容易聯繫的工作場所，就業條例為不斷變化的工作場所[1]，本文選擇了「無邊界工作場所」一詞來喚起和組織行為領域中使用的「無邊界職業」的概念，以及管理領域所討論的「無邊界公司」的概念。[2]僱傭關係、保留或僱用員工提供服務的雇主和其他人員利用一系列電子機制，包括跟蹤器、監聽設備、監控攝影、新陳代謝監測儀和可穿戴技術來監視員工、衡量其績效、避免中斷以及識別、推卸、盜竊或浪費，這些機制可以觀察員工在工作場所內外、工作時間內和工作後的每次活動，其中所收集的數據通過人工智慧演算法轉換為電子簡歷。

本文介紹人工智慧和電子數據收集在工作場所的傳播所帶來的發展影響和危險或威脅等。

在第一部分中，我們將討論在人力資源 (Human Resources) 實踐中日益增多的人工智慧和電子數據收集，在描述了人工智慧的巨大潛力和許多用途之後，我們描述人工智慧在工作場所的使用如何改變僱傭關係、評估、補償和解僱員工工作的做法並收集人工智慧操作所需數據的新類型電子設備。

在第二部分中，我們分析了從人力資源導向的人工智慧無形網路中產生的法律問題，這些網路日益遍及無遠弗屆的工作場所中。具體來說，我們關注人工智慧威脅破壞員工保護的法律領域：反歧視法、隱私法和勞工法，人工智慧在保護員工和促進工作場所司法方面對工會的挑戰。

第三部分，美國勞工法及相關法規範，並且對於未來法律研究提出相關政策規定與建議。

貳、人工智慧與電子監控

一、以演算法成立的人力資源

係因人工智慧無所不在，不論在家裡或是在路上 (例如自動駕駛汽車)，現在越來

1. See generally Katherine V.W. Stone, FROM WIDGETS TO DIGITS: EMPLOYMENT REGULATION FOR THE CHANGING WORKPLACE (Cambridge Univ. Press, 2004).
2. See also Katherine V.W. Stone, Legal Protections for Atypical Employees: Employment Law for Workers Without Workplaces and Employees without Employers, 27 BERKELEY J. EMPLOY. & LAB. L. 251-286 (2006); Katherine V.W. Stone, A Fatal Mis-Match: Employer-Centric Benefits in a Boundaryless Workplace, 11 LEWIS & CLARK L. REV. 451- 480 (2007); Katherine V.W., Employee Representation in the Boundaryless Workplace, 77 CHI.-KENT L. REV. 773-819 (22nd Annual Kenneth M. Piper Lecture) (2002).

越多人工智慧呈現在工作場所，例如它將消除大量工作，創造大量新工作，並改變其他的工作類別，國際律師協會稱人工智慧的發展為第四次工業革命[3]，雇主已經使用人工智慧來篩選工作申請、面試和評估應聘者、跟著員工身體活動、評估績效並建議員工升遷和加薪以及監控員工的電子郵件、電話和非工作時間社交媒體活動。

二、數據演算及深度學習

AI(Artificial Intelligence) 定義為「處理模擬的計算機」，最主要以計算機中的智能行為可以收集並分析大量數據用它來感知、理解、行動和學習，而且學習、模式識別、解決問題和適應不斷變化的環境，其中的關鍵是計算機功率迅速增加和利用它的成本降低，這些預測可用於控制自動駕駛汽車、管理供應鏈以及監控人們的能力、行動和其傾向愛好，從 2015 年到 2017 年，與 AI 相關的併購價值增長了約 26 倍，達到 220 億美元，投資資金引導到數據演算和深度學習、機器人、計算機視覺和語音辨識，存儲的數據量是巨大的並且呈指數級增長。據估計到 2020 年，全球數據量預計將超過 100 zeta 位元組，[4] 這些數據是從多個來源收集來自社交媒體、互聯網搜索和電子支付交易而來的，AI 從過去的購買預測未來想購買下一步或即將推出的商品，甚至在亞馬遜航運專案提出之前已經訂購的商品，其中數據本身可以具有經濟價值 (例如 Facebook 提供手機和其他設備製造商銷售數據)，但最高的價值是分析這些數據，根據可檢測模式預測未來行為，通過使用數據創建一組演算法來嘗試對參數進行模式和類似數量。[5]

三、機器人與人工智慧

機器人在工廠裡很常見，從線輸送帶到機器人武器，使用機器執行任務一向是工廠的主要方向。在 20 世紀 70 年代中期，計算機數控 (Computer Numerical Control；CNC) 機的研製，以擴大使用機器使其任務變化和快速調整[6]。計算機數控使電腦操作人員能夠控制並立即修改，不僅能夠立即完成任務，而且能夠對用於生產的機器進行進給、速度以及定位和速度，使用 AI 啟用的機器人代表了機械化的生產，支援 AI 的機器人可以「學習」新任務，傳統上，軟體工程師對機器人以手臂進行程式完成設計謹慎、精確的任務，例如在汽車車門架上接面板，如果是略有不同的規格的新車模型，手臂必須重新程式設計，然而，AI 允許機械臂自己適應「深度」學習，發生時機器人會有期望的結果，然後使用試驗和錯誤來尋找解決方案。「學習」– 其中多台電腦一起學習，並與每台計算機共用此學習，其他互相學習，所以八隻手臂一起工作可以「學習」一隻手臂可以在八小時內學到什麼，然後可

3. See generally Ajay Agrawal, Joshua Gans, &Avi Goldfarb, Prediction Machines: The Simple Economics of Artificial Intelligence (2018); Paul R. Daugherty & H. James Wilson, Human + Machine: Reimagining Work in the Age of AI (2018).
4. Merriam-Webster,https://www.merriam-webster.com/dictionary/artificial%20intelligence.
5. Gabriel J.X. Dance et al.,Facebook Gave Device Makers Deep Access to Data on Users and Friends, New York Times (June 3, 2018), at https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html.
6. A. Gasparetto, L. Scalera,ABrief History of Industrial Robotics in the 20th Century,8 ADVANCES IN HISTORICAL STUDIES, No. 1 (2019).

以立即分享知識給工廠車間的所有其他機器人，這種「學習」能力使人類和機器人能夠在工廠的地板上一起工作，機械臂可以配備感測器使手臂識別物體，避免與人類發生不安全接觸，和機器人相互補充，例如機器人可以進行重複性的任務，而人做複雜的工作需要獨立的判斷，而這種互補性將遠遠超出工廠在醫療保健等領域的應用。[7]

四、計算機之計算和語音辨識

計算機之計算可以教電腦識別、分類和理解圖像和影像中的內容、模仿和擴展人類視覺系統的行為，現今常見的例子包括一些程式，使自動駕駛汽車能夠區分行人、無生命的物體，或識別對野生動物造成危險的目標，綜上，計算機之計算也使工廠機器人能夠檢測人類員工並避免傷害他們，AI 因此能夠放大人類工作者的身體或感官能力，允許他們做其他不能做的事情，例如使用 Autodesk 的 Dreamcatcher 軟體設計人員根據他們指定的參數創建替代設計系統[8]，這些參數具有功能要求、材料類型、製造方法，AI 可以使計算機能夠從「視覺輸入」中「學習」，它在語音和音訊識別方面也進步迅速，計算機也可以用來分析高噪音環境中的語音，AI 的一些支持者預測 AI 將能夠使用音訊和視頻輸入來分析個人的誠實、情感和個性，AI 在工作場所越來越滲透人類之決定，包括招聘人員之決定、監測性能、預測個人的工作軌跡，評估員工以設定薪酬以及終止僱傭關係的可能性，AI 在工作場所的使用方式，或在不久的將來使用的方式都與法律息息相關。

參、人工智慧在工作場所的偏見問題

一、招募聘僱

消費品公司強生每年收到 120 萬申請 25, 000 個空缺職位，人才招聘公司 HiredScore 提供使用關鍵字搜尋或掃描和排序申請的速度比人快得多，AI 系統可以重新引導申請人可能更適合的空缺職位，或將申請「存檔」，並在其合適工作後通知申請人，[9] 有關招聘人員如何與 AI 合作如何制定超越和搜索應聘者的方法，AI 系統旨在「超越」申請人的簡歷和求職信，以識別可能預測性能的模式，例如技術上和遊戲公司 NVidia 創建內部跟蹤軟體包在申請人身上或檔案上，以致於提交申請人的簡歷在工作上往往表現不佳[10]。

二、就業歧視

在 AI 監控與運作下，歧視和偏見根深蒂固的危險性無所不在，並轉化為運作相當穩定的人力資源，其中可以放大或掩蓋歧視性的偏見，並且有不成比例地排除代表群體

7. Harriet Taylor, Lowe's introduces Lobos, a new autonomous in-store robot, CNBC (Aug. 30, 2016), at https://www.cnbc.com/2016/08/30/lowes-introduces-lowebot-a-new-autonomous-in-store-robot.html.
8. https://autodeskresearch.com/projects/dreamcatcher.
9. See sources cited in David D. Savage & Richard Bales, Video Games in Job Interviews: Using Algorithms to Minimize Discrimination and Unconscious Bias, 32 ABA J. LAB. & EMPLOY. L. 211, 215 nn. 37-42 (2017).
10. Noam Schieber, Unorthodox Hires, and Maybe Lower Pay, New York Times, December 7, 2018.

的員工[11]。另一方面，認為它有可能通過盡量減少或消彌人之判斷，以及通過確定無意間具有排他性的雇傭做法來減少歧視。AI 可以在工作關係的幾個階段進行操作，包括招聘、工資設定、評估、晉陞、紀律和解雇等階段，如果演算法的構建體現邪惡的種族或性別觀念，那麼婦女或有色人種在勞動力市場上將處於嚴重不利地位，此外，使用有關年齡、身心障礙、宗教或其他受保護階級的刻板印象觀念也會發生同樣的情況，然而，如果是產生歧視性結果的演算法，而不是個人的決策者，那麼受到不利影響的員工則無法向法律發起成功的挑戰。[12]

三、偏見如何產生

AI 可以透過多種方式來招募，其中該流程、評估方式、薪酬之計算和紀律流程中容易產生偏見。首先，就像計算機程序一樣 —「輸入，輸出」— 演算法是「偏向，偏出」。例如，通過標記某些文化特定的語音語調，或語音模式，或手勢來分析視頻錄製採訪的演算法，基於種族、族裔、地理出身或社會經濟背景的某些申請人團體，會不成比例地處於不利之地位。更重要的是，演算法的發明者往往依靠雇主過去招募的數據來建構預測的公式[13]，公司複製其最佳員工的模式，因此他們將使用統計上將求職者與這些員工匹配的演算法，如果公司沒有僱用特定類別或分類個人的歷史記錄，則使用過去招聘數據構建的演算法，將系統地將這些人排除在考慮未來空缺職位之外，又例如消防部門幾乎由男性組成，過去招募的數據可能會強調身體素質與耐力相關的重要性；相同地，矽谷長期以來，一直因其以白人男性為主的工作場所而受到批評；基於當前工作場所人口特徵的招聘演算法可能會複製過去的招聘做法，再如 Facebook 等許多在線平台允許廣告客戶和招聘人員根據受眾的興趣定位人口限制受眾偏好和特徵，其中包括基因、性別、宗教和種族。雖然這種演算法偏見通常被視為不同影響的理論，但如該演算法所基於的模型「最佳工作者」是基於歧視性型，產生出演算法可以給出不同待遇歧視的理論。[14]

四、人工智慧減少偏見的潛力

使用 AI 招募會不斷地複製或增加社會上已經存在的真實偏見，例如美國聯邦貿易委員會研究發現，當對個人的名字進行 Google 更有可能產生廣告[15]，暗示針對逮捕

11. G. King & Marko J. Mrkonich, "Big Data" and the Risk of Employment Discrimination, VILL. L. REV. 395 (2018).
12. OKLA. L. REV. 555 (2016); Kevin McGowan, Big Bad Data May Be Triggering Discrimination, BLOOMBERG LAW (Aug. 15, 2016), https://bol.bna.com/big-bad-data-may-be-triggering-discrimination/; Dustin Volz, Silicon Valley Thinks It Has the Answer to Its Diversity Problem, THE ATLANTIC (Sept. 26, 2014), http://www.theatlantic.com/politics/archive/2014/09/silicon-valley-thinks-it-has-the-answer-to-its-diversity-problem/431334/.
13. SeeKim,Auditing Algorithms, (noting that "the law permits theuse of auditing to detect and correct fordiscriminatory bias."). Note, however, that third-party auditing ofonlinealgorithmsmay be prohibited or restricted by current law,making it difficult for academics or researchers to discover bias. See American Civil Liberties Union, Sandvig v. Sessions—Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online(Sept. 12, 2017)(last visited Dec. 20, 2018) (describing litigation challenging the constitutionality of the Computer Fraud and Abuse Act, which makes it a federal crime to access a computer in a manner that "exceeds authorized access").
14. Stephanie Bornstein, Anti discriminatory Algorithms, 70 ALABAMA L.REV. (2019).
15. Saul Hansell,Google Answerto Filling Jobs Is an Algorithm, N.Y. TIMES (Jan. 3, 2007), http://www.nytimes.com/2007/01/03/technology/03google.html?_r=1.

紀錄的人，即使沒有這樣的紀錄存在也可能潛意識說服招聘經理選擇「風險較低的候選人」，此外，採用演算法在操作中仍能產生偏見，例如在研究中，商學院教授安賈和凱薩琳．塔克為 STEMS（Science, Technology, Engineering, Mathematics） 即[16]科學、技術、工程、數學的工作投放了廣告[17]，發現 Facebook 比女性更有可能向男性展示這種廣告，而不是因為 Facebook 演算法作者本身的偏見，由於控制家庭支出比例較高的女性比男性更看重人口，因此，女性廣告收入更昂貴，因此該演算法將廣告定位在男性，其中投資報酬率會更高，演算法簡單地優化原本之成本，廣告投放的方式有效性凸顯歧視性。[18]

肆、人工智慧在工作場所的法律問題

一、員工之隱私權保障

如上所述，公司使用人工智慧收集了大量有關員工的工作生活、習慣和處置等之資訊，這些資訊可能會影響他們整個職業生涯的就業前景，電子監控和監控引發了涉及員工隱私的潛在法律問題，有幾個聯邦和州法規以及普通法理論提到某些方面保護員工的隱私，但所有法規都不足以解決人工智慧和電子監控提出的問題[19]。聯邦法規中包括電子通信隱私法 (Electronic Communications Privacy Act；ECPA)，其中有一、《竊聽法》和二、《存儲通信法》(Save Communication Act；SCA) 和《計算機欺詐和濫用》（Computer Fraud and Abuse Act；CFAA）中有 12 個州有法規禁止，未經各方同意記錄談話，保護員工免受隱私權侵犯的能力，《竊聽法》在防止雇主監督方面適法性，因為它只禁止截取電子資訊，而不允許獲取已經傳輸的資訊[20]，它不適用於一方當事人同意的內文，如雇主擁有電子郵件或通信系統，則視為員工已同意。

再者，《竊聽法》不適用於其他形式如全球定位系統 (Global Positioning System，簡稱 GPS) (和設備以及電子穿戴設備的監測，[21] EPCA《存儲通信法》(SCA)) 保護員工隱私的能力也受到限制，SCA 保護第三方在電子存儲個人私人通信內容[22]，雖然 SCA 沒有明確提及社交媒體帳戶，但此類帳戶屬於法規對電子存儲的定義。公開提供的社交媒體內容可能不受 SCA 的保護，因為此類內容不被視為「私有」內容，另一方面，私下共享的內容，即僅發送給特定群體，或使用限制公眾訪問的隱私設置，可能受到保護，因此雇主的監控會違反法

16. STEM 教育即是科學（Science）、科技（Technology）、工程（Engineering）及數學（Mthematics）四個範疇的縮寫
17. AnjaLambrecht&Catherine Tucker, Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads, available athttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260.
18. Pauline T. Kim,Data-Driven Discrimination at Work, 58 WM.&MARYL.REV. 857, 857 (2017).
19. See, WilliamA. Herbert,The Electronic Workplace: To Live Outside the LawYouMustBeHonest, 12 EMPLOYEERTS.&EMP.POL'Y J. 49 (2008); Robert Sprague,Survey of (Mostly Outdated) LawsAffecting Workplace Monitoring, 93 CHI-KENT LREV221 (2018).
20. IfoemaAjunwa, Kate Crawford, & Jason Schultz,LimitlessWorker Surveillance, 105 CAL.L.REV.736, 2017 (Limitless Surveillance)
21. 18 U.S.C. §.2510 et. seq. (2012).
22. SeeCrispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

規。[23]然而，有相當大的相反見解，第一，對於《規約》而言，「電子儲存」存在相互矛盾的看法，有些法院認為一旦閱讀電子郵件或電子通信，它將不再儲存，因此不在法規範圍內。此外，法院不同意規約的例外適用。例如 Fraser v. Nationwide，在全國範圍內，第三，巡迴法庭認為雇主搜索員工的電子郵件並不違反 SCA，因《美國法》第 2701(c)(1) 條中的 SCA，「由提供有線或電子通訊服務或實體授權的電子郵件的扣押除外」。在這種情況下，電子郵件存儲在雇主自己的伺服器上，因此沒有違規。員工監控也受到質疑，認為違反《計算機欺詐和濫用法》(CFAA)，該法規對未經授權計算的個人造成民事和刑事違法行為，但該法規被解釋為允許雇主在將數據存儲於雇主自己的計算機或網路上時訪問員工的電子資訊。總體而言，面對目前使用的眾多雇主監控和監控工具，現行聯邦法律是保護員工的隱私權。[24]人工智慧在精細化個人數據收集方面的潛力引發一種幽靈，即它將用來創造類似於中國「社會信用」評分的標準，中國的社會信用評分是政府根據政治忠誠 (抗議導致分數較低)、及時償還債務和花過多時間玩電腦遊戲來分析，分配給中國公民波動的數位，分數可用於旅行、學校和政府工作。數據收集和人工智慧資料庫是否會在美國創建永久的電子簡歷，既不能逃脫也不能受到挑戰，其中有待觀察，該答案取決於幾個尚未解決的法律問題，首先，員工對有關他們的數據擁有所有權嗎？如是這樣，在什麼情況下，人們可以排除其他人看到或使用它？第二、如果沒有，人們有權改變數據嗎？第三、他們是否對與其他公司 (如潛在的雇主) 共享這些數據有無任何保護？還是他們的數據與電子簡歷一起旅行，人們既看不到也不能反駁？第四、如果員工的數據不正確，並且數據用於不利的僱傭行為或與其他人員共享時，人們可以有權請求損害賠償嗎？舉例說明潛在的問題，如上所述，HireVue 製作並分析招聘先前面試，以確定對應聘者進行評估。

法律上，HireVue 擁有這些視頻之所有權，就像 Facebook 辯稱自己擁有其所有權，或者至少有使用權，使用者和 Google 提供的使用者生成數據，擁有其平臺上收集的數據。根據歐洲數據隱私權法，相關的回應可能是否定的，但在美國是無效的數據隱私權法，反之，HireVue 的隱私政策解釋說它收集、保留和存儲個人自願提供的申請人資訊，或者從第三方來源或雇主那裡收集的資訊，它還從申請人針對自己的設備或 Cookie 或其他技術跟蹤設備收集數據資料，HireVue 進一步指出，個人有權要求刪除數據，但它不保證任何此類請求都將得到審查及核准，事實上，它有可能創建一個「申請人配置檔」，而且終生保存，故只要有糟糕面試的紀錄，則會因此使求職者的生活前景黯淡。

二、勞工法問題

AI 除了在歧視問題、隱私權法下提出

23. AvnerLevin, &AlissaDelRiego,Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee, 49 AM.BUS. L.J. 63, 83, 87 (2012).

24. Jack Karsten& Darrell M. West,China's social credit system spreads to more daily transactions, BROOKINGS(June 18, 2018), at https://www.brookings.edu/blog/techtank/2018/06/18/chinas-social-credit-system-spreads-to-more-daily-transactions/.

的問題外，在工作場所使用 AI 也可能會產生一些勞工法問題，例如第一，電子監控何時侵犯了勞動者在勞工法下從事互助與保護的一致活動之基本權利？第二，如果存在工會的情形下，人們有權協商討論談判等餘地嗎？關於在工作場所使用 AI 或獲取有關安裝的資訊，在人力資源決策中使用 AI 可行嗎？第三，使用 AI 監控和演算法來決定相關決策，如何影響工會在申訴程式或集體談判中有效代表員工的能力？下面將討論這些問題：

1. AI 和協調保護活動 : 美國之《國家勞動關係法》核心條款是該法的第 7 條[25]，它規定員工有權從事「互助和保護的協同活動」，第 7 條被最高法院和國家勞動關係委員會 (National labor relations board；NLRB) 解釋為保護員工免受解僱或其他制裁之重要依據，當他們從事任何集體行動以改善其員工地位[26]，其中第 7 條保護是為了確保員工能夠自由地討論他們的工作條件，並確定他們是否希望參與集體談判，工作條件包括工資、工時、工作場所條件、就業政策和做法、主管，在某些情況下還包括客戶[27]。
2. 更有甚者，其中第 7 條的保護廣泛適用於兩名或兩名以上員工採取的行動，以及為使他人參加工會、組織或參加工作場所抗議，或以其他方式試圖向雇主施加達成調解的壓力，以實現與工作有關的目標而採取行動。因此，如雇主因討論或就工作場所問題採取集體行動而懲罰員工，或企圖恐嚇或壓制員工這樣做的努力，則違反了勞工法[28]。另外，行動限制或「冷卻」這些活動的雇主會進行不公平的勞動實踐，對於例如雇主社交媒體政策禁止員工使用 Facebook，在上面抱怨他們的工作，這將違反第 7 條中任何雇主搜尋其員工的社交媒體網站，以確定是否有單一或多個員工參與工會活動。有採取許多應對的方法，如員工在第 7 條主張的權利與雇主通過監測和監視來收集數據，以開發或實施支援 AI 的人員管理的努力發生衝突。然而 100 多年來，雇主一直試圖監控他們的員工，以阻止集體行動、識別和找出「麻煩製造者」，他們利用公司間諜和隱藏的攝影機，將滲透器插入員工團體，以檢測和阻止員工的集體行動。隨著 1935 年，NLRB 頒布雇主的監視策略經常受到質疑，認為這些策略干涉員工的第 7 條權利[29]。
3. 董事會認為它違反了雇主進行監視的

25. 29 U.S.C. § 158.

26. George H. Pike,Social Media and the Workplace,31 #9INFORMATION TODAY, at 1 (Nov. 2014).

27. Edward M. Cramp,Annotation, Validity, Construction, and Operation ofState Blacklisting Statutes, 95 A.L.R.5th 1 (2002). A list of these statutes can be found at 1POLICIES AND PRACTICES(HRSERIES) § 60:2 (2019).

28. SettlementAgreement, In re Am. Med. Response ofConn., Inc., No. 34-CA-12576(N.L.R.B. Feb. 7, 2011), available atwww.minnesotaemploymentlawreport.com/NLRB%20Facebook%20Settlement.pdf (settlement of case involving employee who had posted remarks on Facebook angrily implying that her supervisorwasmentally ill and disparaging himwith expletives).

29. See, e.g., NLRB v. City Disposals Systems, 465 U.S. 822 (1984).

影像或造成監視的印象，以便發現和壓制員工受保護的第 7 條活動。因此，例如主管觀察參加工會大廳工會會議的員工觀察是否罷工是非法的[30]。再來，審計委員會認為雇主造成監視的印象是違反的，檢驗員工是否會從陳述中合理地假設他們的工會活動已被置於監視之下[31]。當然並非所有雇主收集的資訊都是非法的，雇主有很多合法的理由來監督他們的員工，例如他們可能想要選擇或員工的位置，以防止在工作上游蕩 (「偷時間」) 或確保員工不從事被禁止的行為，如偷竊、竊取商業機密、在工作期間觀看色情內容等等，出於安全原因，他們還可以進行監控，以確保員工不會進入危險區域，並確保陌生人不會進入工作場所，他們可能還希望監控員工的工作，以便獎勵出色的績效、促進更大的努力或跟蹤個人改進，當監督具有合法目的，但也可能觀察或冷卻受保護的集體行動時，委員會會考慮雇主的合法目的是否超過對員工第 7 條權利所採用的具體手段所承受的負擔[32]。

4. 自 20 世紀以來，亦即 1920 年代起，雇主對員工進行民意調查，經常受到質疑的監控形式涉及對員工態度的一種民意調查顯示，以確定是否有士氣問題並聽取改進建議。[33]這些雖然是合法的且達到合法目的，但投票的方式變相地用來確定哪些員工可能支援工會運動，或恐嚇潛在的工會支援者保持沉默或不活動時，就會發現這種行動是非法的。[34]事實上，NLRB 已經超越明確的民意測驗，當雇主採取行動迫使員工做出「可觀察的選擇」或以其他方式公開表示對工會的支持或反對時，就發現有違規行為[35]。
5. 雇主監控的另一種常見形式是使用隱藏性攝影之鏡頭，雇主經常安裝類似攝影之鏡頭，以防止員工偷竊或逃避工作，相機可以識別相關危險條件，並進行安全干預，這些考量是合理的，並不違反法規，但監控攝影之鏡頭還可以監視員工的組織活動、糾察線或其他受保護的行為，因此NLRB 考慮何時使用隱蔽的監控攝影之鏡頭干擾員工參與互助和保護協調活動的權利，在美國相關案例中，審計委員會認為「雇主在從事受保護的協同活動時，在沒有正當理由的情況下，對員工進行拍照構成非法監視[36]」。
6. 然而，有些案例認為雇主可以在不違反該法律的情況下拍攝或錄影於其工廠外的某些活動，而不能違反該法

30. Ivy Steel& Wire, Inc.,346 NLRB No. 41 (N.L.R.B.),346 NLRB 404 (2006).
31. Sanford M. Jacoby, Employee Attitude Surveys in Historical Perspective, 27 Indus. Rels. 74, 75 (1988).
32. See, e.g. Grand Canyon Education, Inc., 359 NLRB No. 164 (N.L.R.B.), 359 NLRB 1481(2013).
33. Sanford M. Jacoby, Employee Attitude Surveys in Historical Perspective, 27 Indus. Rels. 74, 75 (1988).
34. See, e.g. Grand Canyon Education, Inc., 359 NLRB No. 164 (N.L.R.B.), 359 NLRB 1481 (2013).
35. See, e.g. Allegheny Ludlum Corp.,333 N.L.R.B. No. 109, 2001 WL 855870 (Mar. 30, 2001), enf'd Allegheny Ludlum v NLRB, 301 F.3d 167 (3rd Cir. 2002).
36. Brunswick Hospital Center, 265 NLRB No. 112 (N.L.R.B.), 265 NLRB 803, 807 (1982). See also Dynatron/Bondo Corporation, 323 NLRB No. 217 (N.L.R.B.), 323 NLRB 1263, 1269 (1997).

律，以便為這活動確立合法目的。[37]為確定特定監視事件的合法性，NLRB考慮雇主是否使用監視針對涉嫌參與工會活動的特定個人，或者雇主是否根據工會的推動改變了其監視級別和類型[38]，委員會指出「雖然雇主可以在其財產上或附近觀察公開的工會活動，但雇主不得採取不尋常的行動，讓員工覺得其應保障的活動受到監視，[39]除此之外，委員會解釋說：非法監視是否發生取決於其觀察的性質和持續時間，易言之，主管對從事公司財產公開第 7 條活動的員工的例行觀察不構成非法監視，但雇主在調查從事第 7 條活動的員工時，違反其第 8 條 (a) 項 (1) 款，即以「不常」的方式觀察他們的行為，從而發現他們的非法活動[40]。

7. 在 20 世紀後期，雇主開始使用卡車上的 GPS 跟蹤裝置和辦公室的監控軟體來監控員工的上班活動，追蹤者指出員工是否在浪費上班的時間，以及他們工作上是否符合生產標準，然而，該 GPS 跟蹤裝置經常遭到工會的反對，最主要的理由是這些裝置具有侵入性和壓迫性，通常不會發現這種裝置會不合理地影響非工會工作場所的第 7 條活動。[41]然而，委員會的結論是使用這種裝置確實干擾第 7 條的權利，因為該條文用來追蹤參與組織活動的特定個人的動向。[42]此外，審計委員會還認為在有工會的情況下，安裝 GPS 可構成工作條件的改變，其中同時亦必須遵守相關強制性義務。
8. 監視方法於現今對員工第 7 條權利的威脅甚至比老式的民意調查、攝影機、甚至基本的 GPS 跟蹤器都更大，電子徽章、手機應用、RFID、可穿戴設備和其他 AI 增強型監控設備可用於提高生產率或防止盜竊等合法目的，但也可用於傾聽員工對話、記錄員工移動、監控生物反應和識別員工聚會參與者這些用途，使雇主能夠查明工會支援者並恐嚇他人，如上所述，NLRB 堅持認為監視或造成監視的印象，是非法干涉第 7 條的權利，除非有「合法理由」超過監視的脅迫性質，然而，該標準引出何為「正當理由」如何權衡理事會在平衡時的因素的問題，在 AI 和管理分析時代，雇主對員工行蹤、談話、社交網路、下班活動以及員工的個人習慣、興趣、傾向和情緒的詳細數據收集是否被發現違反勞工法，以及在多大程度仍不得而知。畢竟，談話的設

37. Lechmere, Inc., 295 NLRB No. 15 (1989).
38. See, e.g. Caterpillar Inc., 322 NLRB 674 (1996).
39. Sprain Brook Manor Nursing Home, 351 NLRB No. 75 (N.L.R.B.), 351 NLRB 1190, 1191 (2007). Cf.Intertype Polymer Corp.,Petitionerv.NLRB, 801 F.3d 224 (4thCir,2015).
40. Aladdin Gaming, LLC, 345 NLRB 585 (2005).
41. See e.g. Csc Holdings, Llc and Communications WorkersofAmerica,Case No. 29-CA-190108(NY 2018).
42. NLRBAdvice Memorandum, East Coast MechanicalContractors, 22-CA-253245 (Feb. 6,2003).

備可以比任何公司間諜更有效地了解工會談話，此外，使用生物標誌物和肢體語言來識別哪些員工對工作不滿意，運用 AI 的演算法可以預測哪些員工可能成為工會支援者或只是麻煩製造者，電子監察的這些用途，肯定對員工第 7 條的權利構成威脅。

9. 迄今為止，沒有案件考慮使用先進的監測和 AI，甚至出於合法效率的目的違反勞工法，然而，有些案例涉及相關問題例如雇主是否可以監控員工電子郵件、社交媒體、紅白帖子以及工作場所裡或外面的活動。[43]目前用人單位對員工網上活動監控的合法性在不斷變化，2010 年 11 月 NLRB 對一名雇主提出告訴，指控其解僱一名在 Facebook 網頁上貶低該公司的員工。[44]委員會堅持認為，根據勞工法該職位應該是受到保障的，雖然此案最終得到解僱，但直到最近委員會一直堅持認為員工的社交媒體類似紅白帖等等是受保護的活動，雇主不得在沒有重要理由的情況下干涉這些活動，例如在 2015 年，董事會認為雇主不能維持限制員工在社交媒體上討論公司能力的政策，在 Boch 進口公司中，它指出公司的社交媒體規則要求員工在發佈有關受訪者、受訪者業務或政策問題的評論時必須表明身份，這規範過於空泛，因為員工會合理地解釋該規則，以涵蓋有關其僱傭條款和條件，而自我識別要求將合理地干擾他們在各種社交媒體中的受保護活動，然而，最近的兩項決定表明審計委員會可能很快改變立場，轉而允許雇主限制和監測員工的電子通信[45]。

10. 在 2014 年間，董事會在傳播委員會舉行[46]，認為雇主不能禁止員工將公司電子郵件系統用於與工作無關的目的，包括工會通信。在凱撒娛樂公司裡，董事會邀請所有感興趣的阿米奇提交關於通信是否應被否決的問題，雇主監管員工電子郵件和其他電子通信的標準是什麼，它採用的標準是否也應當適用於對員工使用即時消息、簡訊、社交媒體上紅白帖邀請函之管制？[47]大多數評論員認為，對簡報的呼籲意味著董事會對雇主電子通信政策的管制，至少在工作場所是重大倒退。董事會要求重新審議通信，這是根據 2017 年 12 月 14 日波音公司 (Boeing Corp.) 一案中作出的決定[48]，該裁決認為雇主可以維持無攝影像機之規則，包括 (1) 禁止在其場所使用手機，即使該規定干擾

43. NLRB Advice Memo, BP Exploration of Alaska, Inc.Case 19-CA-29566 (July 11, 2005).
44. See David Bayer, Employers Are Not Friends With Facebook: How The Nlrb Is Protecting Employees' Social Media Activity, 7 Brook. J. Corp. Fin. & Com. L. 169, 174 (2012).
45. Boch Imports,362 NLRB No. 83at707 (2015); aff'd sub nom Boch Imports, Inc.v NLRB,826 F.3d 558(1stCir., 2016).
46. Purple Communications, 361 NLRB No. 126 (2014).
47. 2018 WL 3703476(August 1, 2018).
48. The Boeing Co., 365 NLRBNo. 154 (December 14, 2017).

和 / 或可能冷卻員工的保護活動。(2) 根據工會活動頒布的規則 ; 或 (3) 該規則已適用於限制行使第 7 條權利，然麥克法倫議員指出的反對意見表示該「文明規則」不存在[49]。

11. 首先，大多數人沒有真正嘗試來界定「文明的基本標準」是什麼？特別是工作場所的標準是什麼？再者，在每一個工作場所環境中，它們真的一樣嗎？建築工地和醫院一樣？在裝卸碼頭和零售商店一樣？其次，大多數人似乎忽視了根據《國家勞動關係法》所開展的共同形式的受保護協調活動可以合理地理解為不文明，為了抗議不安全的工作條件而離開工作是否符合「基本文明標準」？或者分發那些用不禮貌的語言、批評雇主不向員工支付所欠工資，並敦促員工抵制的文章？多數人顯然決定允許所有雇主維持任何他們想要的「文明」規則，而忽視各種工作場所可能發生的勞資糾紛的現實，並讓員工採取行動為自己辯護，就像聯邦勞工法意旨相同。

12. 以高露潔 - 帕爾莫利夫公司為例，董事會認為雇主必須與工會就隱藏監控攝影像頭的放置問題進行討論協商，因為使用這種攝影像頭與凱撒娛樂公司有關，而波音公司的案例表明目前的董事會可能會批准雇主對員工的電子通信進行廣泛監控，以便他們可以監管新授權的文明規則，如果是這樣，勞工法不會成為對員工在線活動的廣泛監控和監控的障礙，監控可用於收集數據以用於支援 AI 的員工評估。

13. 根據勞工法，有多數代表工會發揮相當的功能[50]，雇主不能單方面改變現有的工資、工時和工作條件，而不首先與工會談判到僵局之困境。如上所述，雇主有相當大的自由從事監視和監測，如果它這樣做的合法目的，也就是說，一旦工會獲得認證，雇主必須與工會就監控攝影的使用和放置問題進行討論[51]。工作條件的變化，有協商討論的必要性，從邏輯上而言，同樣的理由也適用於其他跟蹤器和生物監測器的安裝，它們也會承擔談判義務，在這種情況下，在實施與 AI 相關的監測之前，雇主需要與工會談判協商。

14. 舉例而言，在化學溶劑公司裡，雇主安裝監控裝置工會反對的相機，NLRB 因此而裁定說明在沒有與工會進行首次談判的情況下這樣做是違反法律的[52]。它指出發現被調查者的立場沒有說服意義，很難接受這樣的命題與隱藏的攝影機和對工作環境的潛在影響，員工對攝影機的關注程度要小。事實上相反。至少放置了一

49. Citing Lutheran Heritage Village – Livonia, 343 NLRB 646 (2004).

50. 58 U.S.C. 158(a)(5).

51. NLRB v. Katz, 369 U.S. 736 (1962).

52. NLRB v. Wooster Div. of Borg-Warner Corp, 356 U.S. 342 (1958).

些攝影機導致員工經常使用的設施觀察區域，雖然法院不反對被告之論點，即新攝影機與國土安全部建議的安全措施一樣，但受訪者沒有表明國土安全部需要特定數量的新攝影機或其特定位置，撇開這些問題不談，其他問題也可以提出來，或在談判期間討論，如攝影機的大小或其用途，最好能傳達給員工，因此，不能接受被調查者的總結結論是「協調協商是徒勞無益」的。因此，在此本文的結論是被申請人違反第 8(a)(5) 條和 (1) 單方面安裝新的監控攝影機，而無需向歐盟提供，且事先通知協商的機會。

伍、結論與建議

然而，支持監控攝影機和談判義務的案件，GPS 追蹤器可能不適用於所有類型的電子監控，原因有二：首先，如果發現這些設備是「強制性的談判主體」，則只有談判義務，其他監控設備的問題還只是個懸而未決的問題，第二，即使這類裝置被確定為強制性談判的主體，談判義務也只要求雇主在與工會談判至陷入僵局之前不得採用這些裝置，一旦陷入僵局，雇主必須允許實施其提議來修改。

另一個會出現的問題是，雇主是否必須談判協商使用 AI 演算法來指導它有關紀律、工作分配或晉陞的決策，還有其中涉及員工查看和質疑任何員工之忠誠度等問題，AI 增強人員查看信息的結論及權利，對於這些問題與安裝電子監測設備一樣，結果將取決於這些協定是否是強制性談判的主體，聯盟在演算法決策中的代表，工會代表員工處理相關問題和談判協定，在這當中，它們都需要獲得通過電子監測收集的資訊，以及在雇主決策中實施執行 AI 的過程。

在此，最高法院認為工會有權獲得參與有意義的談判所必需的資訊，為增強談判義務，工會必須要求提供資訊，且必須表明這些資訊是工會在談判中提出及討論，藉由向工會提供有關雇主的做法，以及有關為談判目的，使用 AI 進行人事管理決策未來計劃的資訊，工會可以有談判籌碼，要求提高使用 AI 的透明度，並限制監視的範圍和用途，與談判一樣，工會還需要獲得 AI 資訊，以便在申訴程式中有效地代表員工，當作使用電子監控和 AI 演算法來檢測員工不當行為時，代表員工的工會將尋求駁斥指控或減輕處罰，例如幾乎所有集體談判協定都限制雇主解僱員工的權利，但雇主有「有權利」這樣做，只是原因標準是模糊和無限的，案件往往由仲裁員決定，然而，要確定是否有真正的原因，工會需要知道是什麼，通知有爭議的決定，雇主可能決定解僱生產率低於平均水準的員工，理由是他不相信員工會改善，預測可能是 AI 評估員工過去和現在的生活標記和情緒狀態的結果，工會需要瞭解所有這些因素如何融入評估，以便有效地評估及應對。

參考文獻

1. Katherine V.W. Stone, FROM WIDGETS TO DIGITS: EMPLOYMENT REGULATION FOR THE CHANGING WORKPLACE (Cambridge Univ. Press, 2004).

2. Katherine V.W. Stone, Legal Protections for Atypical Employees: Employment Law for Workers Without Workplaces and Employees without Employers, 27 BERKELEY J. EMPLOY. & LAB. L. 251-286 (2006); Katherine V.W. Stone, A Fatal Mis-Match: Employer-Centric Benefits in a Boundaryless Workplace, 11 LEWIS & CLARK L. REV. 451- 480 (2007); Katherine V.W., Employee Representation in the Boundaryless Workplace, 77 CHI.-KENT L. REV. 773- 819 (22nd Annual Kenneth M. Piper Lecture) (2002).
3. Ajay Agrawal, Joshua Gans, &Avi Goldfarb, Prediction Machines: The Simple Economics of Artificial Intelligence (2018); Paul R. Daugherty & H. James Wilson, Human + Machine: Reimagining Work in the Age of AI (2018).
4. Gabriel J.X. Dance et al.,Facebook Gave Device Makers Deep Access to Data on Users and Friends, New York Times (June 3, 2018)
5. A. Gasparetto, L. Scalera,ABrief History of Industrial Robotics in the 20th Century, 8 ADVANCES IN HISTORICAL STUDIES, No. 1 (2019).
6. Harriet Taylor, Lowe's introduces Lobos, a new autonomous in-store robot, CNBC (Aug. 30, 2016).
7. David D. Savage & Richard Bales, Video Games in Job Interviews: Using Algorithms to Minimize Discrimination and Unconscious Bias, 32 ABA J. LAB. & EMPLOY. L. 211, 215 nn. 37- 42 (2017).
8. Noam Schieber, Unorthodox Hires, and Maybe Lower Pay, New York Times, December 7, 2018.
9. G. King & Marko J. Mrkonich, "Big Data" and the Risk of Employment Discrimination, VILL. L. REV. 395 (2018).
10. OKLA. L. REV. 555 (2016); Kevin McGowan, Big Bad Data May Be Triggering Discrimination, BLOOMBERG LAW (Aug. 15, 2016)
11. https://bol.bna.com/big-bad-data-may-be-triggering-discrimination/; Dustin Volz, Silicon Valley Thinks It Has the Answer to Its Diversity Problem, THE ATLANTIC (Sept. 26, 2014),
12. Kim,Auditing Algorithms, (noting that "the law permits theuse of auditing to detect and correct fordiscriminatory bias."). Note, however, that third-party auditing ofonlinealgorithmsmay be prohibited or restricted by current law,making it difficult for academics or researchers to discover bias. See American Civil Liberties Union, Sandvig v. Sessions—Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online(Sept. 12, 2017) (last visited Dec. 20, 2018) (describing litigation challenging the constitutionality of the Computer Fraud and Abuse Act, which makes it a federal crime to access a computer in a manner that "exceeds authorized access").
13. Stephanie Bornstein, Anti discriminatory Algorithms, 70 ALABAMA L.REV. (2019) .
14. Saul Hansell,GoogleAnswerto Filling

Jobs Is an Algorithm, N.Y. TIMES (Jan. 3, 2007), http://www.nytimes.com/ 2007/ 01/ 03/ technology/ 03google.html?_r= 1.

15. AnjaLambrecht&Catherine Tucker, Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads, available athttps://papers.ssrn.com/sol 3/papers.cfm?abstract_id= 2852260.

16. Pauline T. Kim,Data-Driven Discrimination at Work, 58 WM.&MARYL.REV. 857, 857 (2017).

17. WilliamA. Herbert,The Electronic Workplace: To Live Outside the LawYouMustBeHonest, 12 EMPLOYEERTS.&EMP.POL'Y J. 49 (2008); Robert Sprague,Survey of (Mostly Outdated) LawsAffecting Workplace Monitoring, 93 CHI-KENT LREV 221 (2018).

18. Sanford M. Jacoby, Employee Attitude Surveys in Historical Perspective, 27 Indus. Rels. 74, 75 (1988).

19. Grand Canyon Education, Inc., 359 NLRB No. 164 (N.L.R.B.), 359 NLRB 1481 (2013).

20. Allegheny Ludlum Corp., 333 N.L.R.B. No. 109, 2001 WL 855870 (Mar. 30, 2001), enf ' d Allegheny Ludlum v NLRB, 301 F. 3d 167 (3rd Cir. 2002).

21. Brunswick Hospital Center, 265 NLRB No. 112 (N.L.R.B.), 265 NLRB 803, 807 (1982). See also Dynatron/Bondo Corporation, 323 NLRB No. 217 (N.L.R.B.), 323 NLRB 1263, 1269 (1997).

22. Lechmere, Inc., 295 NLRB No. 15 (1989).

23. Caterpillar Inc., 322 NLRB 674 (1996).

24. Sprain Brook Manor Nursing Home, 351 NLRB No. 75 (N.L.R.B.), 351 NLRB 1190, 1191 (2007). Cf.Intertype Polymer Corp.,Petitionerv.NLRB, 801 F. 3d 224 (4thCir, 2015).

25. Aladdin Gaming, LLC, 345 NLRB 585 (2005).

26. Csc Holdings, Llc and Communications WorkersofAmerica,Case No. 29-CA- 190108(NY 2018).

27. NLRBAdvice Memorandum, East Coast MechanicalContractors, 22-CA- 253245 (Feb. 6, 2003).

28. NLRB Advice Memo, BP Exploration of Alaska, Inc.Case 19-CA- 29566 (July 11, 2005).

29. David Bayer, Employers Are Not Friends With Facebook: How The Nlrb Is Protecting Employees' Social Media Activity, 7 Brook. J. Corp. Fin. & Com. L. 169, 174 (2012).

30. Boch Imports, 362 NLRB No. 83at 707 (2015); aff ' d sub nom Boch Imports, Inc.v NLRB, 826 F. 3d 558(1stCir., 2016).

31. Purple Communications, 361 NLRB No. 126 (2014).

32. 2018 WL 3703476(August 1, 2018).

33. The Boeing Co., 365 NLRBNo. 154 (December 14, 2017).

34. Citing Lutheran Heritage Village–Livonia, 343 NLRB 646 (2004).

35. 58 U.S.C. 158(a)(5).

36. NLRB v. Katz, 369 U.S. 736 (1962).

37. NLRB v. Wooster Div. of Borg-Warner Corp, 356 U.S. 342 (1958).

行動App 安全風險評估與防範措施之研究

A Study on Mobile App Security Risk Assessment and Preventive Measures

賴森堂
實踐大學資訊科技與管理學系 助理教授
E-mail:stlai@g2.usc.edu.tw

摘　要

資訊與網路技術快速成長，各種網路應用環境普及且融入人們日常生活，透過行動 App 可以達到互動、溝通、支付及交易等行為，搭配行動裝置的便利性，行動 App 已成為網路應用必備的工具。行動 App 依應用可區分為三種類型：無須使用身分鑑別 (純功能性)、須使用身分鑑別 (具認證功能與連網行為)、具交易行為等。各類型行動 App 取得方便，只要提供相關資料即可在多項行動裝置下載、安裝與使用，不過，台灣地區每天有超過 4000 多部手機中毒或遭駭客入侵，嚴重者可能造成民眾個資外洩與財務損失。為了降低使用行動 App 帶來的安全風險，本文蒐集 App 多方面資訊，以行動 App 安全事證為基礎，設計一套行動 App 安全風險評估 (MASRA) 程序，適時評估 App 的安全風險，有效協助民眾篩選高安全性的 App，及時提醒民眾採取安全防範措施，保護民眾個資隱私與財產安全，避免敏感性資料外洩與財務損失。

關鍵字：行動 App、安全事證、MASRA、防範措施、行動裝置。

Abstract

Information and network technologies are growing rapidly, and various network

application environments are popularized and integrated into people's daily lives. Through mobile apps, interaction, communication, payment, and transactions can be achieved. With the convenience of mobile devices, mobile apps have become a necessary tool for network applications. Mobile apps can be divided into three types according to applications: purely functional, with authentication function and connection behavior, with financial transaction function, etc. All types of mobile apps are easy to get. People can download, install and use on multiple mobile devices as long as you provide relevant information. However, more than 4000 mobile phones are poisoned or hacked every day in Taiwan, and severe cases may cause personal information leakage and financial losses. In order to reduce the security risks caused by the use of mobile apps, this paper collects various information about the apps. Based on the security evidence of the mobile apps, designs a Mobile Apps Security Risk Assessment (MASRA) procedures to assess the security risks of the apps in a timely manner and effectively assist the people to select high-security apps. MASRA can also promptly remind the people to take security precautions to protect the privacy of personal information and property security and to avoid the leakage of sensitive information and financial losses.

Keywords: Mobile App, Security certificate, MASRA, Preventive measures, Mobile devices.

壹、緒論

無線通訊的行動裝置已成為人們活動的必備工具，行動 App 的應用大幅提升企業與組織的營運效率與服務品質，增強市場的競爭優勢，也為人們帶來高度便利性與優質的生活，不過，網路環境卻存在許多待克服的挑戰，包括數據品質、處理效能、網路傳送速度、持續擴充能力及資訊安全等議題 (O'Loughlin, 2019)，其中，又以資訊安全議題衝擊最大也是民眾最關注的項目 (Zhu, 2014)。行動裝置安裝 App 可以達成多樣化的應用，資策會產業情報研究所（MIC）2015 年進行「行動 App 消費者調查分析」發現，每天使用的 App 類型，以「社交通訊類（80. 9%）」最高，其次為「行動遊戲類（35. 3%）」、生活服務和資訊類（31. 8%）、影音媒體（30. 1%）」(MIC, 2016)。其中，社交通訊類 App 的使用者需提供身分鑑別，發行單位可以利用使用者個資及通訊相關資料，風險較高，至於其他須付費的知名 App 安全性相對較高。此外企業與組織為了擴展市場、增加客戶來源，以提升市場競爭優勢，紛紛推出搭配優惠、集點及促銷等活動的行動 App，提供民眾免費下載與安裝，適時達到行銷的效益。下載行動 App 一般需要提供敏感性的個資，而網路傳輸過程經常是資訊被竊取的關鍵，企業與組織發行的行動 App 應該完成安全檢測且通

過嚴格的滲透測試，以善盡保護用戶的個人資訊安全。資訊設備及網路技術持續快速演進，政府相關單位與國家安全機構無法全面配合行動 App 應用，制定出新的安全條款與規範，很難有效檢測與具體管控行動 App 的安全性，使得行動 App 運作環境存在待改善的安全風險。

一般民眾申請銀行帳號、手機門號、信用卡或是學校入學都必須提供完整的個人資料，以便確認客戶或學生的真實身份。這些個資可以協助檢、警、調處理相關犯罪事件的調查作業，不過，「個資保護法」對於個資與敏感性資料蒐集、處理及利用有嚴格的規範，甚至要求蒐集民眾個資與敏感性資料的組織或機構必須導入一套資訊安全管理系統 (ISMS) 如 ISO 27001, BS 7799，且善盡保護個人資料安全的責任，以避免個資與敏感性資料外洩，遭到濫用，造成民眾的困擾與損失。現今的行動 App 功能廣泛，許多民營企業或組織為了提升市場競爭力且增加營收，在未明確告知的情況下，以優惠與集點促銷方式吸引民眾下載且安裝行動 App。不過，大部份的 App 沒有取得安全標章也沒有通過安全檢測，App 可能存在許多安全缺失與漏洞，行動裝置有被惡意程式或駭客入侵的風險。行動 App 的安全問題與缺失，可能形成資安事件，對一般民眾可能造成的衝擊與影響包括暴露個人行蹤隱私、個人生活習性成為蒐集對象、個人健康狀態外洩成為醫療藥品行銷對象，以及關鍵個資與敏感性資料外洩被不當利用等，這些狀況除了會困擾民眾日常生活外，更可能進一步造成民眾難以預期的精神與財務損失。下載與使用行動 App 必須注意安全風險。

全球知名串流影音平台 Netflix 是民眾欣賞影片常用的平台，日前有一款惡意 App –「FlixOnline」宣稱可以免費看兩個月 Netflix，有民眾下載後，裝置的 WhatsApp 遭入侵，導致信用卡、銀行帳號等資料外流，受害民眾已有 500 多人 (林妍湊，2021)。最嚴重的情況是當裝置被駭客入侵後，一般民眾根本無法立即察覺，企業或組織更不會主動告知，直到民眾發現個資或敏感性資料被不當利用，為時已晚。為此，本文以 App 安全事證為基礎，探究行動 App 安全風險評估方式，進而規劃一套行動 App 安全風險評估 (Mobile App Security Risk Assessment; MASRA) 程序與防護措施，主動確認行動 App 的安全風險，適時提醒民眾採取安全防範與保護措施，以保護民眾個人資料安全。第二節針對行動 App 安全問題及安全制度之建立進行探討。第三節以安全性的角度，整理行動 App 的三種類型及關鍵的安全事證，且規劃出四個行動 App 的安全等級與使用建議。第四節以行動 App 安全事證為依據，提出 MASRA 作業流程與防護措施。第五節評估行動 App 安全防護措施的效益。第六節再次強調保護個人資料安全的重要性，及 MASRA 程序與防護措施的貢獻，且針對本主題作結論。

貳、行動App潛在的安全風險與安全規範

行動 App 的應用非常廣泛且與民眾的日常生活息息相關，使用安全的行動 App 是民眾最在意的議題，值得深入探究。

一、行動 App 安全問題之探討

國內手機的普及率逐年增加，2018 年的

調查報告中，用戶數已超越 2, 925 萬戶 (國家發展委員會，2019)，隨著資訊技術與應用環境持續的演進，行動裝置結合 5G 網路技術大幅提升數據傳輸的效率，使得行動 App 的應用更多元且廣泛，大幅增加行動 App 的運用範疇。不過，許多 App 開發商並沒有引用「安全開發指引」進行設計與開發，發行前也沒有通過完整的測試與安全檢測等作業，造成駭客與惡意程式入侵裝置，散播廣告訊息、盜取個人關鍵資料等，困擾且侵犯用戶的使用安全。近期幾起行動 App 的資安事件中，出現惡意程式入侵及個人資料外洩的案例，衝擊用戶的隱私與日常生活。由於行動 App 的發行單位，幾乎採取委外開發，受到經費有限、時程較短，因此，經常會以功能優先為導向，忽略行動 App 安全開發指引應考量的項目，一旦發生資安事件，對於發行單位的企業或組織反而造成負面影響。一般民眾對於行動 App 的安全性缺乏明確的認知，三成以上的用戶不清楚 App 業者蒐集個人資訊的用途 (國家發展委員會，2019)，更不知道如何保護行動裝置內部存放資料的安全。本文以疫情期間，QR Code 實聯制掃描器下載為例，實聯制掃描器可以協助民眾進出賣場、銀行等公共場所，此項 App 被下載次數已達幾百萬次。不過，一篇報導標題為：「熱門條碼掃描器 App 一夕間變成惡意軟體，上百萬 Android 手機遭木馬入侵」(科技新報，2021)，表示極少數的民眾會關注掃描器 App 是否取得安全標章、是否通過安全檢測、由哪一家開發商製造、由哪家公司或組織發行等。大多數民眾也不知道掃描器 App 屬於哪一類型 App，可能遭遇哪些安全風險。一旦 App 發生被駭客或惡意程式入侵等資安事件，可能對民眾帶來難以預期的衝擊與損失。從上述案例可以瞭解用戶對行動應用 App 缺乏安全性認知：

(一)不知道行動應用 App 的用途與類型：一般用戶不確定下載行動 App 所屬的功能與類型，更不知道使用此類型 App 可能帶來的安全風險，因此，一旦行動 App 發生資安事件，將無法適時採取保護措施以降低個人資料外洩的風險。

(二)不知道行動應用 App 的發行單位：民眾經常透過他人推薦、廣告信件、廠商優惠或促銷活動的誘惑下，非主動取得行動 App。因此，很少注意行動 App 的發行單位，更不瞭解行動 App 是由那個單位開發的，下載且使用來路不明的行動 App 存在高度的安全風險。

(三)不知道行動應用 App 是否曾發生資安事件：行動 App 存在安全漏洞或缺失、開發商或發行單位缺乏一套安全管理制度都可能會發生資安事件，民眾下載且安裝 App 前，極少會注意行動應用 App 是否曾發生資安事件。

(四)不在意行動應用 App 是否通過安全檢測：涉及金融交易或網路存付款行為的行動 App 屬於高風險類型，應該進一步確認 App 是否取得 MAS 安全標章或通過安全檢測機制。

此外為了改善行動 App 運作的安全危機，應該從開發商、發行單位、政府 / 資安機構及一般使用者等四方面各自承擔其責任：

1. 行動 App 開發商的責任：行動 App 分析設計初期，就必須將 App 安全品質納入考量，參與產品設計與開發的

團隊必須接受資訊安全訓練課程，且遵循安全開發指引。App 發行前，除了進行各項功能性、品質、效能等測試外 (Wasserman, 2010)，還必須以 OWAPS 訂定的十大風險 (OWASP, 2020)，完成安全性的檢測作業。

2. 行動 App 發行單位的責任：蒐集行動 App 用戶資訊的企業與組織應導入資訊安全管理制度，對蒐集的用戶個資須善盡保護的責任，嚴格管控網路安全與行動 App 的後端伺服器，且依 ISMS 的要求，每半年進行一次弱點掃瞄，每年進行一次滲透測試，以確保用戶資訊的安全性。
3. 一般使用者的責任：下載、使用行動 App 前，應了解使用 App 的安全風險，如果無法確定行動 App 的安全性，就應該拒絕下載與安裝。對於需要提供個資或屬於金融交易等高風險類型的 App，下載安裝前更應該小心防範。此外使用者於行動裝置安裝檢測工具與防毒軟體，也可以降低行動 App 安全風險。
4. 政府或資安機構的責任：資安機構應針對 App 安全設計、開發、檢測與發行等活動制定相關的規範，以保障民眾使用行動 App 的安全。

二、MAS 安全標章與行動 App 安全規範之探討

經濟部工業局基於民眾關切使用行動應用 App 等資安議題需要，於 103 年 10 月委託資策會成立工作小組，於 105 年 2 月依序完成「行動應用 App」的資安規範、資安檢測基準、及安全開發指引，引導行動應用 App 開發商導入資安概念。105 年 11 月正式成立「行動應用資安 (MAS) 聯盟 」，以推動我國行動應用 App 相關產業發展，提升國內行動應用 App 資訊安全 (行動應用資安聯盟，2017)。經濟部工業局制訂「 行動應用 App 基本資安規範 」，並由財團法人全國認證基金會 」(Taiwan Accreditation Foundation, TAF) 認可的檢測實驗室，受理 App 開發商的檢測申請，確保開發之 App 符合資安檢測基準要求。MAS 聯盟於 107 年 10 月更新行動應用 App 基本資安檢測基準版本，將初級 / 中級 / 高級變更為甲類 / 乙類 / 丙類。改版的重點將原來的分類分級制度，改以行動應用程式之性質分類不分級 (行動應用資安聯盟，2019)。MAS 聯盟與 TAF 推動的「 行動應用 App 基本資安標章 」(Mobile Application Basic Security，以下簡稱 MAS 標章) 可以提升民眾行動裝置的安全性 (資訊月，2020)。

除了經濟部工業局推動的「 行動應用 App 基本資安規範 」與檢測機制，一些知名的 App 商店、金融機構及政府單位也規範 App 上架或發行的審核與確認準則，經過審核或確認後的 App 具有較高的安全性，民眾可安心使用，規範說明如下 :

(一) 蘋果公司於 2010 年發布了應用程式稽核指南：該指南屬於可隨時更新的檔案，規範應用程式不得包含具有攻擊性，敏感等內容。蘋果公司根據該指南稽核每個 App，通過後可在 App Store 上販售 (Apple Store, 2021)。Apple 強調其 App Store 是探索和下載 app 安全可靠的地方，其中非常重要的就是確保他們提供的 app 符合隱私、安全和內容的最高標準。確實如此，在 App Store 上架的

行動應用 App 都必須經過完整的安全檢測，因此，從 App Store 下載的行動應用 App 多了一層安全保障。

(二)Google Play Store 強調為所有人提供安全可靠的使用體驗：Google Play 制定相關政策為了 App 和遊戲安全地提供給全世界的使用者。App 開發商必須瀏覽 Google Play 政策的相關資訊、詳閱《開發人員發行協議》，才能符合 Google 政策，在 Play Store 上販售產品 (Google play，2021)。

(三)金融機構發行行動 App 的安全政策：中華民國銀行商業同業公會全國聯合會為確保金融機構提供客戶使用之行動 App 之資訊安全，除符合經濟部工業局「行動應用 App 基本資安規範」外，應具有一致性安全控管作業，並保障消費者權益。只要是電子支付業者或銀行業者等機構發行的 App，都會直接受到電子支付專法 / 銀行法條列規範 (金新聞稿，2020) 的要求，每年都需要將發行的 App 送檢驗且取得證書或標章，因此下載金融機構發行的 App 是相對安全的。

(四)政府單位的行動 App 安全規範都採取經濟部工業局制訂的「行動應用 App 基本資安規範」，開發過程建議採用「行動應用 App」的資安規範、資安檢測基準、及安全開發指引，發行前應取得對應等級的 MAS 標章，但是，此規範並沒有強制性的要求。

參、行動App的類型與關鍵的安全事證

本節將探討行動 App 類型及關鍵的安全事證，有效確認行動 App 類型，可以識別安全事證的關鍵性。

一、行動 App 的類型

行動 App 的種類繁多，用途、功能與特質也有很大的差異，且不斷有新的產品推出，所以不可能針對個別的行動 App 提出不同的防護措施，此外不同用途的行動 App 對於民眾的安全威脅也不盡相同，因此必須先了解行動 App 的功能與特性，才能採取適當的安全防護措施。經濟部工業局委託資策會完成的 App 基本資安規範將行動 App 依安全風險定義成三個類型 (iT 邦幫忙 , 2020)，本文則將民眾較常安裝使用的行動 App 分成：不需提供個資的單機 App、瀏覽 / 遊戲 App 及金融交易與行動支付 App 等三種類型，以資安規範的三個類型結合民眾使用 App 的種類說明如下：

(一)第一類型 App，無須使用者身分鑑別之行動 App：

大部分民眾使用的 App 屬於第一類，通常都是查尋工具 (如公車到站時間、氣象資料、統一發票兌獎)，可以融入日常生活，提升活動便利性。此類型 App 採用的資料通常是開源資料 (Open Data)，安全風險相較低，所以資安層級可以不用太高，不過，App 仍須防範駭客與惡意程式的入侵。

(二)第二類型 App，須使用者身分鑑別之 動 App：

民眾經常使用的通訊、社群、影音平台等軟體與網購 App 都屬於此類型，需要透過民眾提供的個資確認用戶身分。因此，這類型 App 會使用到個人敏感性資料，開發商應針對交付前的 App 進行安全檢測且取得安全標章，發行單位存放個資的伺服器需要具備安全的管理機制，以保護用戶個資與敏感性資料的安全。

(三)第三類型 App，含有交易行為之行動 App：

此類型 App 具有處理金流交易行為，屬於安全風險最高的行動 App，一旦發生資安事件對於民眾的衝擊與損失最大 (Wang, 2016)。只要是電子支付業者或銀行業者等機構發行的 App，都會直接受到電子支付專法 / 銀行法條列規範的要求 (金新聞稿 , 2020)，每年都需要將發行的 App 送檢驗且取得證書或 MAS 丙類安全標章。因此，開發商務必導入安全開發指引，發行單位務必送檢驗且取得檢測證明且通過 MAS 丙類安全標章，以確保 App 的安全性，下載金融機構發行的 App 是相對安全的。

另外還有一個特殊類型是公家機關發行的 App，公家機關的 App 大都採取委外開發 (outsourcing)，開發合約會要求開發商必須引用安全軟體發指引進行設計與開發，完成的 App 必須取得相對等級的 MAS 安全標章與檢測證書。將各類型 App 的安全風險與相關單位職責匯集成一關係表 (參閱表 1 所示)。

表 1. 不同類型 App 的風險與單位職責關係表（本研究整理）

單位職責 App 類型	安全風險	開發商 / 發行單位		發行單位具備安全管理制度
		取得 MAS 安全標章或檢測證書	導入安全軟體開發指引	
第一類型	中等	V		
第二類型	高	V	V	V
第三類型	最高	V	V	V

二、行動 App 的關鍵安全事證

一般民眾對於行動 App 的來源不重視也缺乏 App 安全的關鍵知識，因此對於行動 App 的安全風險很難具體改善，本文蒐集行動 App 四個層面的安全事證做為行動 App 安全風險評估的依據：

(一)行動 App 發行單位為金融機構或具審核機制的平台之事證：國內金融機構或知名販售平台 (如 App Store, Google Play Store 等) 對於發行或上架的行動 App 會明確的規範或採取嚴格的審核機制以確認 App 的安全性。行動 App 一旦發生資安事件或出現異常狀況，也會立即採取下架或封鎖措施。因此，下載使用此類型行動 App，對於使用者的安全性

具有一定保障。

(二)行動 App 取得安全標章或通過安全檢測是關鍵且重要的事證：通過 TAF 的 MAS 後，可以申請行動應用資安聯盟提供行動 App 安全標章 (MAS 標章)，具公信力的檢測實驗室檢測通過的行動 App 可確定 App 的安全性。

(三)管理行動 App 用戶資料是否導入 ISMS 制度或制定嚴謹的安全管理機制：ISMS 是一套國際化標準組織 (ISO) 制訂的資訊安全管理制度，可以提升 App 用戶資料安全。不過，網路上許多 App 管理單位為了管理方便而忽略了安全性，管理系統完全沒有設定使用者權限，缺乏安全的管制措施，有心人士也可以利用安全管制不足的系統進行資料竊取、竄改與濫用等惡意行為。因此，應該避免使用未導入 ISMS 制度或缺乏安全管理制度的行動 App。

(四)App 發生資安事件或被封鎖、下架是值得注意的安全評等項目：行動 App 或 App 用戶個資管理單位發生被入侵、被濫用或資料被竊取等資安事件，造成個資與敏感性資料外洩，用戶受到難以估計的損失。因此，資安事件也是安全評等的項目。本文引用具高可靠度的兩項網路資安事件資訊，其中國家資通安全通報應變網站 (https://www.ncert.nat.gov.tw/#) 會不定期公布國內外發生的資安 (事件) 新聞，iThome 新聞網每一或兩個月發布十大資安新聞 (周峻佑，2020)。被販售平台封鎖或下架的 App 也必須注意其安全風險。

本文依上述的四項安全事證，對行動 App 的安全等級進行評估，將行動 App 分成 4 個等級，說明如下 (參閱表 2 所示)：

1. 高安全等級：行動 App 發行單位為金融機構或具審核機制的平台，且行動 App 取得安全標章、開發商及發行單位都取得 ISMS 證照或具安全管理制度，App 也不曾發生未即時改善的資安事件者屬於高安全等級，可安心使用。
2. 安全等級：行動 App 發行單位為金融機構或具審核機制的平台，而行動 App 取得安全標章或開發商及發行單位取得資訊安全制度證照、App 無不良風評且不曾發生未即時改善的資安事件者屬於安全等級，可使用。
3. 可接受等級：行動 App 發行單位為金融機構或具審核機制的平台，而安全標章、ISMS 認證或安全管理機制可以視為選擇項，不可以發生未改善的資安事件者屬於可接受等級，需小心可使用。
4. 危險等級：行動 App、開發商或發行單位曾經發生資安事件且未採取適時的改善措施者都屬於此等級，強烈建議不要下載與使用，如果已經下載使用的 App，應該立即從裝置中移除。

表 2. 行動 App 分成 4 個安全等級（本研究整理）

安全等級	發行單位為金融機構或具審核機制的平台	取得安全標章或安全檢測認證	通過 ISMS 認證或具備安全管理制度	曾發生資安事件 (未即時改善)	使用建議
高安全	V	V	V		可放心使用
安全	V	至少取得一項證照或制度			可使用
可接受	V	可選擇	可選擇		小心使用
危險				V	不建議使用 (使用中應立即移除)

肆、行動App安全評估與防護流程

確定行動 App 的用途與來源，才能採取適當的安全防護措施，本節以行動 App 的安全標章為依據擬訂行動 App 安裝與應用的安全防護流程。

一、行動 App 安全風險評估程序與防護流程

取得行動 App 的用途、功能、安全措施與發行單位等關鍵事證，才能判斷其安全等級，且針對有安全風險的行動 App 採取適當的防護措施。本文設計的 MASRA 程序分為七個步驟 (參閱圖 1) 包括蒐集四項安全事證、識別行動 App 所屬的類型、評定行動 App 的安全等級，採取安全防範方式與保護措施等，運作流程說明如下：

步驟 (一) 確認 App 發行單位為金融機構或具審核機制的平台之事證：

許多機構或販售平台會明確的規範或採取嚴格的審核機制以確保發行或上架的行動 App 已達安全的等級。此外，當行動 App 發生資安事件或出現異常狀況，會立即採取下架或封鎖措施。因此，下載使用此類型行動 App，對於使用者的安全性具有一定保障。

步驟 (二) 以行動 App 的應用與功能，識別行動 App 所屬的類型：

行動 App 的應用與功能對於用戶會有不同層次的安全威脅，因此行動 App 安全風險評估應該先識別行動 App 的類型。若行動 App 屬於第二或第三類型，則必須取得更關鍵的安全事證，以評估行動 App 的安全風險。

步驟 (三) 查證行動 App 取得安全標章或通過安全檢測之事證：

進入 MAS 聯盟可以搜查取得安全標章的行動 App 及發行單位或開發商的資料。行動 App 屬於第一類型則應取得

MAS 甲類安全標章，第二類型則應取得 MAS 乙類安全標章，第三類型則應取得 MAS 丙類安全標章。確認行動 App 取得的安全標章可以進一步評估行動 App 的安全風險。

步驟 (四) 確認 App 管理單位取得 ISMS 證照或具備安全管理制度之事證：

若行動 App 屬於第二或第三類型，則必須透過網路爬蟲搜尋關鍵行動 App 名稱、行動 App 開發商與發行單位的安全管理制度及 ISMS 證照等事證，包括：

1. 檢視 App 管理單位是否建制一套 ISMS 制度。
2. 搜集用戶個資的企業或組織是否建制一套資料安全管理制度。

步驟 (五) 透過高公信度網站搜尋行動 App 發生資安事件或被封鎖下架之事證：

確認行動 App 或發行單位是否曾發生資安事件或被販售平台封鎖下架的 App。本文引用具高可靠度的兩項網路資安事件資訊，其中國家資通安全通報應變網站會不定期公布國內外發生的資安 (事件) 新聞。

步驟 (六) 剖析與評定行動 App 的安全等級：

取得行動 App 四項安全事證與 App 類型，再依 3. 2 節安全等級評定方式為基礎，區分行動 App 的安全等級，且建議使用高安全與安全等級之行動 App。其中一旦發現企業、組織、開發商或行動 App 本身曾經發生資安事件且未即時改善者，將強烈建議不要下載或直接移除此行動 App。

步驟 (七) 完成行動 App 安全風險評估後，列出可採取的安全防範方式與保護措施。

下一節將依評定的行動 App 安全等級，說明可採取的適當安全防範方式與保護措施。

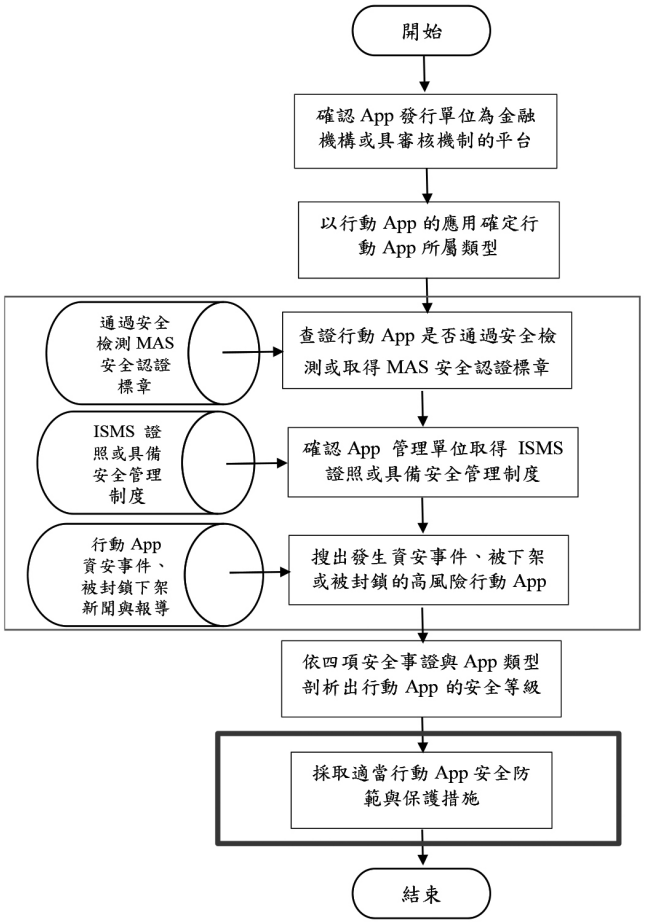


圖 1. MASRA 的運作流程圖（本研究整理）

二、行動 App 防範與保護措施

為了讓民眾能夠安心使用行動 App，減少行動 App 安全風險的威脅，建議民眾可以採取兩方面的防護措施 (參閱表 3 所示)：

(一)下載安裝行動 App 的前置處理作業，必須採取行動 App 安全風險防範方式：

1.確認下載行動 App 的用途、功能及必要性。

2.確認行動 App 是否取得安全標章或已通過安全檢測。

3.若是屬於第二或第三類型的行動 App，還必須判斷行動 App 的發行單位或後台的管理機構是否取得 ISMS 證照且具備一套持續維護系統運作安全的資訊安全管理制度。

4.隨時注意欲下載的行動 App、開發商、發行單位或管理機構是否曾發生資安事件且未能立即改善。

5.須使用者身分鑑別或含交易行為之行動 App 屬於高風險的行動 App，絕對要確認開發商與發行單位。

(二)行動 App 安全風險保護措施：下載安裝行動 App 的後續處理作業

1.針對已安裝且經常使用的行動 App 應隨時進行 App 安全檢視與安全確認作業，且更新為最新的安全版本。

2.一旦發現行動 App 存在不適用的高風險或發生資安事件應盡快移除。

3.行動 App 已有一段時間 (6 個月) 未使用，應盡可能移除此行動 App，若有提供個資也應要求發行單位必須刪除個資與敏感性資料。

表 3. 不同類型 App 等級要求及採取的防護措施（本研究整理）

行動 App 類型	安全等級要求	確認發行單位	安全防範方式	保護措施
第一類型： 無須使用者身分鑑別	• 可接受 • 安全 • 高安全	有登記的單位	• 至少取得 MAS 甲級標章 • 留意資安事件與評價	• 不用時，應移除
第二類型： 須使用者身分鑑別	• 安全 • 高安全	知名機構或企業	• 取得 MAS 乙級或丙級標章 • 未發生資安事件 / 已修補資安缺失 • 已導入 ISMS 或具安全管理制度	• 注意個資、隱私及敏感性資料的使用與安全性
第三類型： 含有交易行為	• 高安全	金融機構或具審核機制平台	• 取得 MAS 丙級標章 • 未發生資安事件 / 已修補資安缺失 • 已導入 ISMS 或具安全管理制度	• 注意個資、隱私及敏感性資料的使用與安全性 • 隨時配合發行單位更新安全版本

伍、MASRA程序的效益分析

有一篇文章曾提到「下載 App 前先看評價和留言」，主要的目的就是要提醒民眾不要隨意下載或使用來路不明的 App，本文認為只看評價和留言是不夠的，除了要留意已經發生的資安事件外，還必須了解 App 的功能與類型、App 是否取得安全標章或通過安全檢測等，下載 App 是否須要提供個人資料，發行單位與開發商是否取得 ISMS 認證等相關事證。對於一般民眾很難適時取得完整的資訊，更不知如何評估行動 App 的安全風險。為此，本文以安全事證為基礎，規劃一套 MASRA 程序，首先識別行動 App 的類型、開發商 / 發行單位的安全管理措施，再從多項安全事證確認行動 App 的安全等級，結合多項安全事證用來評估行動 App 的安全風險，且依安全等級建議採取適當的防範方式

提升行動 App 使用安全。不過，環境的變遷，資訊技術持續演進，各行各業不斷推出新的行動 App，受限於現實的條件，絕大部分的行動 App 並沒有通過安全檢測也未取得 MAS 安全標章，行動 App 的安全事證並不易取得，因此，初期先以行動 App 的安全管理措施、是否曾經發生資安事件、發行單位的信譽及開發商是否導入資訊安全管理制度為評估行動 App 安全等級的關鍵項目。當輿論與民眾對行動 App 安全有進一步的認知與要求後，將促使政府單位與相關機構制定標準的行動 App 安全規範，此階段將帶動各種行動 App 的安全標章與認證制度，對本研究提出的行動 App 安全防護措施勢必帶來更具體且完整的效益。本文規劃的 MASRA 程序與防範措施，具體的成果說明如下：

一、 分析一般民眾對行動 App 的安全風險缺乏認知

二、 行動 App 安全檢測與安全標章制度建立之現況探討

三、 整理衝擊行動 App 安全風險的安全事證

四、 結合 App 類型與各項安全事證，規劃出四種安全等級的 App 及使用建議

五、 具體提醒民眾下載高風險行動 App 應該關注的安全項目與細節

一般用戶下載行動 App 前，可能會透過看評價和留言、留意發行單位、是否提供個資及是否通過安全檢測且取得安全標章來評估行動 App 的安全風險，這些評估方式都只能確認其中部分的安全事證 (參閱表 4 所示)，無法達到全面性的評估，本文規劃的 MASRA 作業程序可以全面性的評估各項行動 App 的安全事證，具體保護民眾關鍵資訊安全與個人隱私。

表 4. 評估方式與安全事證對照關係表（本研究整理）

評估方式 / 安全事證	看評價與留言	留意發行 / 開發單位	是否需要提供個資	檢視安全檢測與標章名冊	MASRA 作業程序
資安事件 (未立即改善)	V				V
通過安全檢測				V	V
取得安全標章				V	V
具備 ISMS 制度		V	V		V
具備安全管理制度		V	V		V

本文規劃的 MASRA 程序已完成多項安全事證的蒐集，制定四種安全等級評的估方式，且針對不同安全等級的行動 App，列出多項安全防範與保護措施，結合網路爬蟲模組的數據取得與分析作業 (參閱圖 2 所示)，促使 MASRA 程序已具備開發成工具的優勢。

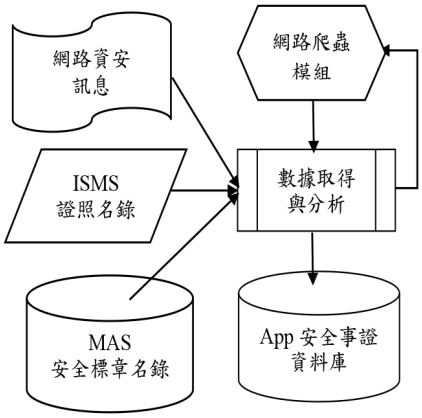


圖 2. 結合網路爬蟲的安全事證取得與分析作業（本研究整理）

陸、結論

行動裝置的普及率愈來愈高，而行動 App 強化了行動裝置的便利性與應用範疇，已成為人們日常生活必備的工具，多元的應用與便利性卻也隱含了用戶許多的安全風險。本文以行動 App 多項安全事證為基礎，提出一套 MASRA 作業流程，建議採取適時的防範方式與保護措施降低行動 App 的安全風險。本文將行動 App 的安全品質分為高安全、安全、可接受與危險等四個安全等級，針對不同類型 App 及取得的安全事證給予安全風險評等且提供用戶適當的使用建議。當民眾對行動 App 安全風險有進一步的認識與要求後，可促使政府單位與資安機構強制要求開發商必須導入行動 App 安全規範與開發指引，交付前必須通過安全檢測作業或取得 MAS 安全標章，具體且有效提升民眾使用行動 App 的安全性。對本文提出的 MASRA 程序與防護措施勢必帶來更具體且完善的效益。本文規劃的 MASRA 程序，具體的優勢說明如下：

一、 下載、使用來路不明的行動 App 對個人資訊與隱私安全可能的衝擊

二、 探討知名 App 商店、金融機構發行的行動 App 安全規範與 MAS 聯盟安全標章制度建立

三、 評估 App 的四個安全等級且適時提供使用者防護建議

四、 具體提高民眾對行動 App 安全議題的重視與認知

五、 保護民眾行動裝置關鍵資訊安全與個人隱私

參考文獻

1. 產業情報研究所，2016，行動 App 消費者調查，資策會，2016/ 2/ 2
   https://mic.iii.org.tw/news.aspx?id= 423
2. 林妍湊，2021 惡意程式冒充免費 Netflix 程式，藉 WhatsApp 自動回覆功能散布，ithome 網安新聞 (iThome.COM) 。
   https://www.ithome.com.tw/news/ 143705
3. 國家發展委員會，2019，108 持有手機民眾數位機會調查報告，中華民國一〇八年八月

4. 行動應用資安聯盟，2017，行動應用 App 基本資安自主檢測制度介紹，106 年 8 月
5. 行動應用資安聯盟，2019，行動應用 App 基本資安檢測基準 V 2. 1 及 V 3. 0 分類之差異說 , 2019- 03- 06 https://www.mas.org.tw/news_detail.php?id= 69
6. 科技新報，2021，熱門條碼掃描器 App 一夕間變成惡意軟體，上百萬 Android 手機遭木馬入侵，2021- 02- 09 https://technews.tw/ 2021/ 02/ 09/barcode-scanning-app-android-malware/
7. 資訊月，2020，你的手機 APP 安全嗎？「 App 安全認證 」為你的手機安全把關！ https://itmonth.blog/ 2020/ 05/ 28/
8. App Store, 2021, App Store 審核指南 (最近更新日期：2021 年 2 月 1 日)

   https://developer.apple.com/cn/app-store/review/guidelines/
9. Google play，2021，開發人員計畫政策。(2021 年 3 月 1 日生效)

   https://support.google.com/googleplay/android-developer/answer/ 10477564?hl=zh-Hant&ref_topic= 9877065
10. 金新聞稿，2020，管會推動「 金融資安行動方案 」，追求安全便利不中斷的金融服務目標 (更新日期：2020- 08- 06)

    https://www.fsc.gov.tw/ch/home.jsp?id= 96&parentpath= 0, 2&mcustomize=news_view.jsp&dataserno= 202008060003&dtable=News
11. iT 邦幫忙，2020，行動應用基本資安規範，2020- 09- 17

    https://ithelp.ithome.com.tw/articles/ 10238702
12. 周峻佑，2020，2020 年 7 月十大資安新聞，iThome | 2020- 10- 11
13. O'Loughlin, K., Neary, M., Adkins, E. C., & Schueller, S. M. , 2019. Reviewing the data security and privacy policies of mobile apps for depression. Internet interventions, 15, 110- 115.
14. Zhu, H., Xiong, H., Ge, Y., & Chen, E., 2014, Mobile app recommendations with security and privacy awareness, In Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 951- 960).
15. Wang, Y., Hahn, C., & Sutrave, K., 2016, Mobile payment security, threats, and challenges, In 2016 second international conference on mobile and secure services (MobiSecServ) (pp. 1- 5). IEEE
16. Wasserman, A. I., 2010, Software engineering issues for mobile application development. In Proceedings of the FSE/SDP workshop on Future of software engineering research (pp. 397- 400).
17. OWAS, 2020, Top 10 Web Application Security Risks, 2020, May, https://owasp.org/www-project-top-ten/

應用COBIT 2019制定企業治理策略

Employing COBIT 2019 For Enterprise Governance Strategy

作者：Christopher C. Anoruo
CRISC, CISM, CGEIT

譯者:諶家蘭
政治大學會計系教授

戰略是實現既定目標的計劃。 COBIT 2019 旨在幫助從業人員將標準資訊和技術 (I&T) 控制應用於企業治理策略。將控制目標映射到國際標準化組織 (ISO)/ 國際電工委員會 (International Electrotechnical Commission,IEC) 標準 ISO / IEC 27001: 2013 信息安全管理從 COBIT 5 到 COBIT 2019 框架是一項有用的練習，有助於制定治理策略。 映射 ISO 27001: 2013，ISO / IEC 38500: 2015 信息技術 — 本組織的 IT 治理，COBIT 5 和 COBIT 2019 之間的關係，可為從業人員提供績效數據值、見解和結果，而這些資訊有助於戰略管理諮詢和決策。COBIT Focus 中的許多文章對這種關係進行了探討。平衡計分卡 (BSC) 也已成功體現企業資訊科技治理 (EGIT) 的績效衡量的價值。

是什麼推動了這種映射的需求?

「企業資訊科技可以帶來甚麼？」這個問題應該這樣問：「企業資訊科技可以如何應用才能增加價值？」，改變問題可以幫助從業人員專注於企業資訊科技的業務價值，企業資訊科技的成本優化實踐，投資優先級，資訊科技項目融資和資源採購選項，項目收益實現和創新會計。

推動映射練習需求的目標包括：

- 通過映射 COBIT 過程來控制目標，並以此來衡量整體治理和戰略的績效和整合資訊科技治理
- 通過企業資訊科技治理 (EGIT) 來滿足企業對知識創新、有效部署和全面治理和管理的需求
- 開發可應用於組織或業務單位的個人進行評估和職能分配之關鍵績效指標（KPI）

值得注意的是，企業資訊科技的優化

及創新整合會導致數位顛覆，從而推動社會、工業和商業向前發展。然而，過去仍沒有真正的破壞性技術產生，不過出現了大量的創新，而這些創新的想法是基於企業相關的技術應用。

為甚麼治理系統會失敗?

當治理系統實施失敗時，常見的原因之一是它們沒有被啟動，亦沒有進行適當的管理以確保其效益的實現。執行管理層必須是治理計劃發起人並給予其支持；這些治理計劃需要有適當的範圍，並訂立可實現的目標，讓企業能夠按照計劃的步伐適應變化。

如 COBIT 2019 所提到的，企業資訊科技的治理及管理應該要成為整體企業治理和文化的一部分，涵蓋整個業務和企業資訊科技功能性領域。

資訊科技治理需要甚麼?

資訊科技治理研究所 (IT Governance Institute , ITGI) 指出，資訊科技治理主要有兩個目標：資訊科技給企業帶來的價值及減輕資訊科技的風險。

這些目標是由業務推動因素驅動的，例如資訊科技與業務的戰略協調；適當資源支持的資訊科技對企業可靠程度；測量結果，可以確保獲得用於戰略規劃和設定未來績效目標的度量標準。人們無法衡量、無法監控的內容。績效監控有助於進行基準測試。

企業資訊科技治理的 5 個主要目標均由 COBIT 2019 中提到的利害關係人之價值所推動。值得注意的是，其中 2 個推動因素是結果，分別為價值交付及風險管理。其他 3 個主要領域或推動因素是：

1. 策略調整
2. 績效管理
3. 資源管理 (涵蓋所有範圍)

這些主要領域是由內部推動的，因為雖然 EGIT 及企業策略有差異，但他們在同一個生命週期中發展，並且相輔相成，就像治理者確定誰是管理者，而管理者則是被指派負責指導工作及執行決策。

ISO/IEC 38500—資訊科技治理框架

ISO 38500: 2015 包含 6 條指導原則，以實現對 IT 的良好公司治理：

1. 責任
2. 策略
3. 收購
4. 績效
5. 一致性
6. 員工行為及企業文化

若一個企業想要成功發展資訊技術治理，需將資訊技術內化成為文化，而這種文化是建基於策略計劃中傳達明確的目標以及達成可以用績效衡量的可實現目標。在實踐上述 6 個原則時，管理層必須執行三個必須之任務，換言之，員工行為守則需要評量、指導及監測如 COBIT 2019 所描述。

COBIT 2019治理及管理目標

如前所述，本文目的是解構治理流程並提供一個指引以發展可持續的企業策略。COBIT 2019 是一個幫助企業規劃策略及達

成其治理目標的框架，並透過企業有效的資訊科技治理傳達價值。COBIT 2019 中的治理及管理目標分為 5 個範疇，每個領域使用數個動詞作為名稱，以傳達其主要目的及其所包含的目標之活動範圍：

1. 評估，指導及監控 (EDM)
2. 調整，規劃及組織 (APO)
3. 建立，獲取及實施 (BAI)
4. 傳達，服務及支持 (DSS)
5. 監控，評估及衡量 (MEA)

治理目標屬於 EDM 範疇，在這個範疇，治理機構會評估現有的策略選項，指導高級管理層執行已選定策略，監控策略的成效。EDM 涵蓋串聯目標和確認利害關係人的推動因素和需求。

管理目標分為以下四個領域：

- APO— 為企業之資訊科技介紹企業整體 I&T 總體組織、戰略和支援活動。
- BAI— 負責定義資訊科技之問題，並獲取解決方案且實施，並將前述一系列過程進行整合融入至企業日常流程。
- DSS— 提出可實施的資訊科技服務及支援，包括資訊安全服務及支援。
- MEA— 根據內部績效目標、控制目標及外部需求，提出績效監控方案及資訊科技確信。

COBIT 2019 目標級聯

目標級聯讓企業能夠調整目標的優先順序。COBIT 2019 的目標級聯進行了大翻新；在新版本中，企業目標和整體目標已進行合併、減少、更新和重新說明。

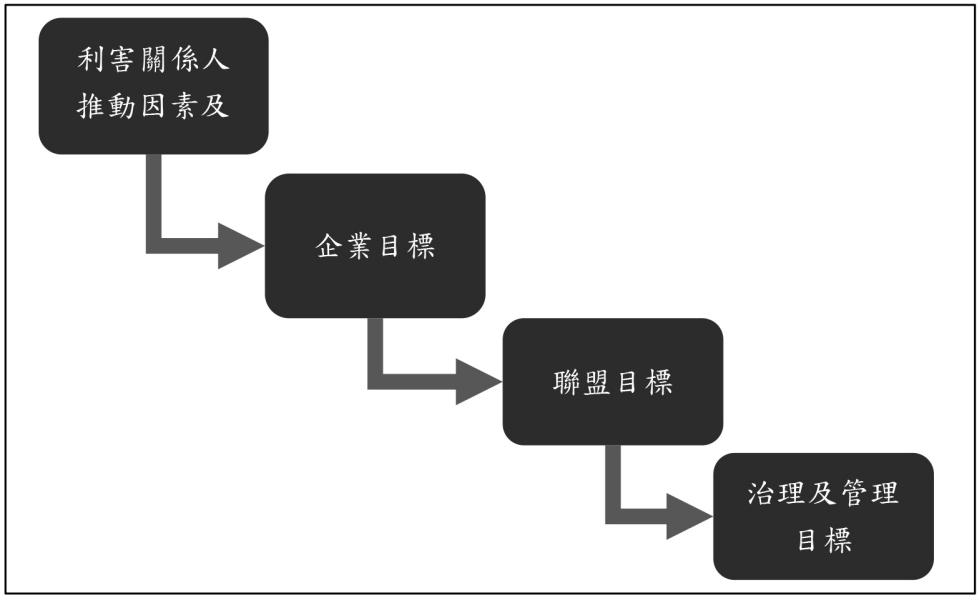


圖 1—COBIT 2019 目標級聯

COBIT 5 和 COBIT 2019 目標級聯的精髓，是在於將資訊科技策略與企業策略相結合。

值得注意的是，COBIT 5 中的目標級聯是與治理和策略有關，並且將利害關係人的需求轉化成量身訂造、可實行的企業目標、資訊科技相關目標及推動目標。但是在 COBIT 2019 裡面，目標級聯支持管理目標，而管理目標是優先考慮企業目標的。

COBIT 2019 中有 13 個企業目標和 13 個聯盟目標，當中沒有額外的資訊科技相關之目標。COBIT 2019 更新及簡化了企業目標和聯盟目標。

COBIT 2019 數位革新和私隱問題框架

COBIT 2019 框架幫助從業人員完善業務和企業 I&T 技能，以識別業務的真正本質，並提供滿足這些需求的技術解決方案。

隨著知識和創新推動技術的發展 , 策略性資訊趨勢顯示出巨大的顛覆性潛力，並為未來 5 年的創新數字顛覆奠定了基礎。企業資訊科技的發展不能忽視這些趨勢。

組織必須檢查這些趨勢對業務的影響，並適當調整業務模式和運營，否則就有可能失去競爭優勢。由於這一系列的演變，數據在這個物聯網時代變得非常重要，而且人工智慧 (AI) 對數據亦有高度的依賴性，企業有必要將之前 COBIT 5 提及的管理數據的 DS 11 轉變為 COBIT 2019 中提及的 APO 014。物聯網、增強實境 (augmented reality ,AR) 和人工智慧這些技術的出現，使數據成為企業的核心資產，甚至在面對網絡犯罪時，數據亦是珍貴的資產。數據管理和數據安全不再是企業運行時的成本，而是維持企業運行的核心組成部分。

應用數據風險中私隱問題之隱憂日漸提升；財務損失；業務中斷；損失或丟失資產；無法合符法規、監管或合約的要求；以及名譽損壞。有效的數據管理可以增加系統的整合，有助於減低風險及降低私隱問題。首席技術長 (CTOs), 首席資訊長 (CIOs) 和企業架構師 (EAs) 應該與首席安全長 (CSOs) 及首席數據長 (CDOs) 合作，使企業接納及適應 COBIT 2019 框架，有策略地運用數位革新。各國政府、城市規劃者及商業領袖必須要重視網絡犯罪之警示，所以在設計和建立到基礎設施管理等等的階段，都應該讓網絡安全專家參與。

最具影響力的破壞性創新會影響社會、工業和商業領域，而不是科技領域。從收音機到影音播放是一個破壞性創新。優步 (Uber) 亦是一個影響社會、工業及企業的破壞性創新，但他並沒有影響到科技。科技創新、變革和破壞性創新都是同樣的意思。數位創新必須長期出現；任何短期的破壞性創新都是一時的。雲端計算並沒有反映出技術的創新，而是重新定義了資源存取的技術。

使用COBIT 5的企業IT控制結果及應用

前面提到 , COBIT 2019 將業務和企業 IT 技術改進，以瞭解業務的真正本質，並提供滿足這些需求的技術解決方案。

建立控制使企業能夠通過使用平衡計分卡方法的實地評估，得出優化 I&T 投資和為利益相關者創造價值的結果。這些結果還點出了 IT 治理的痛點。將 COBIT 4. 1 控制目

標的資料值，映射到 COBIT 5 治理和管理實踐（使用 ISO/IEC 27001: 2013 的資料作為輸入）顯示了 COBIT 5 的 IT 相關過程如何支援每個 IT 相關目標。 此映射使用以下主要（P)和次要（S)關係表示：

- “P”代表主要關係，當有一個重要關係時，即 COBIT 5 流程是實現 IT 相關目標的主要支持。
- “S”代表次要關係，這個關係仍然是強的，但相對不重要，即 COBIT 5 流程是實現 IT 相關目標的次要支持。

COBIT 5 範疇及流程		IT BSC構面資訊及相關技術目標																		
COBIT 5之流程		IT與業務策略的一致性	IT業務的合規性和遵從業務相關法律和監控	執行管理層對IT相關業務的決策	可控的IT相關業務風險	從IT推動的投資和服務組合實現利益	IT成本、收益和風險的轉化	交付與業務需求一致的IT服務	適當地使用應用程序、資訊和技術解決方案	IT敏捷性	資訊安全，審閱基礎設施及應用程序	IT資產、資源及效用最佳化	整合應用及科技於業務流程中，並啟用及支持業務流程	交付提供利益之計劃，需要符合預算、符合要求及質量標準	對決策可靠且有用之資訊的可用性	IT遵從內部政策	具競爭力及積極的業務和IT人員	知識、專業能力和業務創新的積極性		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17		
1	評價、指導及監控	財務						客戶		內部因素							學習和成長		COBIT4.1映射	狀態
EDM01	確保治理框架的設置和維持	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S	85.66	86%
EDM02	確保收益實現	P		S		P	P	P	S		S	S	S	S	S		S	P	87.66	88%
EDM03	確保風險優化	S	S	S	P		P	S	S		P			S	S	P	S	S	84.81	85%
EDM04	確保資源優化	S		S	S	S	S	S	S	P		P		S			P	S	86.99	87%
EDM05	確保對利害關係人之透明度	S	S	P			P	P						S	S	S		S	-	0%
																				69%
2	調整、規劃及組織																			
APO01	管理IT管理框架	P	P	S	S			S		P	S	P	S	S	S	P	P	P	84.48	84%
APO02	管理策略	P		S	S	S		P	S	S		S	S	S	S	S	S	P	86.33	86%
APO03	管理企業架構	P		S	S	S	S	S	S	P	S	P	S		S			S	82.51	83%
APO04	管理創新	S			S	P			P	P		P	S		S			P	84.33	84%
APO05	管理投資組合	P		S	S	P	S	S	S	S		S		P				S	87.33	87%
APO06	管理預算和開支	S		S	S	P	P	S	S			S		S					88.17	88%
APO07	管理人力資源	P	S	S	S			S		S	S	P		P		S	P	P	85.93	86%
APO08	管理關係	P		S	S	S	S	P	S			S	P	S		S	S	P	-	0%
APO09	管理服務協議	S			S	S	S	P	S	S	S	S		S	P	S			82.92	83%
APO10	管理供應商		S		P	S	S	P	S	P	S	S		S	S	S		S	81.39	81%
APO11	管理質量	S	S		S	P		P	S	S		S		P	S	S	S	S	83.46	83%
APO12	管理風險		P		P		P	S	S	S	P			P	S	S	S	S	83.03	83%
APO13	管理安全		P		P		P	S	S		P				P				84.48	84%
																				78%
3	建立、取得及實施																			
BAI01	管理方案和項目	P		S	P	P	S	S	S			S		P			S	S	90.00	90%
BAI02	管理需求定義	P	S	S	S	S		P	S	S	S	S	P	S	S			S	83.82	84%
BAI03	管理解決方案識別及建立	S			S	S		P	S			S	S	S	S			S	82.48	82%
BAI04	管理可用性和能力				S	S		P	S	S		P		S	P			S	80.00	80%
BAI05	管理組織變革啟用	S		S		S		S	P	S		S	S	P				P	84.31	84%
BAI06	管理變革			S	P	S		P	S	S	P	S	S	S	S	S		S	86.50	87%
BAI07	管理面對變更的接受能力及應對				S	S		S	P	S			P	S	S	S		S	85.00	85%
BAI08	管理知識	S				S		S	S	P	S	S			S		S	P	83.61	84%
BAI09	管理資產		S		S		P	S		S	S	P			S	S			82.25	82%
BAI10	管理配置		P		S		S		S	S	S	P			P	S			81.39	81%
																				84%
4	交付、服務和支持																			
DSS01	管理營運		S		P	S		P	S	S	S	P			S	S	S	S	81.62	82%
DSS02	管理服務需求及事項				P			P	S		S				S	S		S	82.64	83%
DSS03	管理問題		S		P	S		P	S	S		P	S		P	S		S	80.00	80%
DSS04	管理連續性	S	S		P	S		P	S	S	S	S	S		P	S	S	S	82.11	82%
DSS05	管理安全服務	S	P		P			S	S		P	S	S		S	S			82.28	82%
DSS06	管理企業流程控制		S		P			P	S		S	S	S		S	S	S	S	80.22	80%
																				81%
5	監控、評價和評估																			
MEA01	監控、評價和評估績效及一致性	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S	80.28	80%
MEA02	監控、評價和評估內部控制系統		P		P		S	S	S		S				S	P		S	85.54	86%
MEA03	監控、評價和評估是否符合外部要求		P		P	S		S			S					S		S	84.21	84%
																				83%
IT BSC構面資訊及相關技術目標		77	84	43	83	87	73	74	85	84	84	83	56	86	82	84	86	75		

圖 2—（輸入 ISO/IEC 27001: 2013 之數據）映射 COBIT 5 治理及管理流程之結果

說明：

- 欄代表了 17 個一般 IT 相關的目標，按照 IT 的平衡計分卡分組
- 列代表的是 37 個 COBIT 5 的流程，根據之前提及的 5 個範圍分組

COBIT 5 的結果如圖 3，如圖所示該框架並沒有充分說明項目管理對 EGIT 的重要性。BAI 和 MEA 有更高的依賴性。不過，COBIT 2019 發現了這些問題並且讓這個框架能夠更容易的被接納及適應。

COBIT 5個領域及流程	得分	未來目標
評價、指導及監控	69%	85%
調整、規劃及組織	78%	90%
建立、取得及實施	84%	95%
交付、服務和支持	81%	90%
監控、評價和評估	83%	90%
	79%	90%

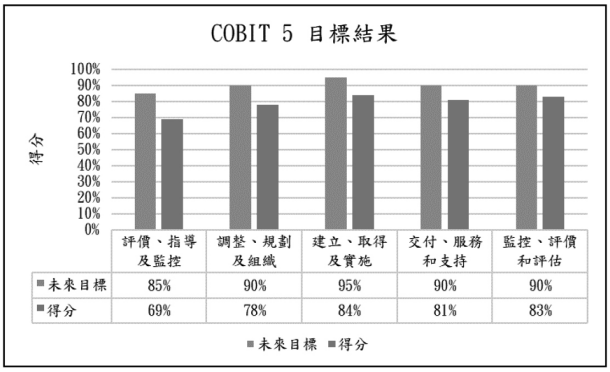


圖 3—BSC 構面價值作為 COBIT 4. 1 及 COBIT 5 控制目標的映射資料值（使用來自 ISO/IEC 27001-2013 的輸入資料 ）的結果

使用COBIT 2019的企業I&T控制的結果與應用

COBIT 5 治理與管理執行（使用來自 ISO / IEC 27001:2013 的輸入數據 ）到 COBIT 2019 治理與管理目標的對映數據值顯示了 COBIT 2019 治理和管理目標如何支持一致性目標。此對映使用 value scale 表示：

- 值“P”指出存在重要關係（即，COBIT 2019 目標對於達成一致目標是主要支持 ）。
- 值“S”指出仍然存在強烈但較不重要的關係（即，COBIT 2019 治理和管理目標是對於一致目標的輔助支持 ）。

可以將評估結果向下鑽取到輸入值，並且可以使用對映值向後查看從 ISO / IEC 27001 控制目標和問題中的一組對映數據中決定得分較低的根本原因；這將成為制定組織所需的行動計劃的基礎。

關於主要價值的假設與觀察

更新會標示黃色（P 和 S）如圖 4 所示：

- 對映表 - 將一致目標對映到 COBIT 2019 治理和管理目標。
- AG 09- 按預算及時交付計劃並滿足需求和品質標準是計劃管理的核心定義，適用於 EGIT。

考慮到這一點，AG 09 應該對 EDM 02 確保收益交付和 DSS 06 管理業務流程控制具有主要支持，因為它們與計劃管理功能存在重要的關係，而當 AG 09 與 EGIT. 有關時，AG 09 應該與 BAI 06 管理 IT 具有次要關係。

COBIT 2019之範圍及流程		將調整目標映射到治理及管理目標														
COBIT 2019架構		IT業務的合規性和支援業務遵從外部法律和監控	可控的IT相關業務風險	從IT推動的投資和服務組合實現利益	財務資訊相關的技術貿量	交付與業務需求一致的IT服務	將商業需求轉換成可實行的解決方案的靈活性	資訊安全，處理基礎設施、應用程序以及穩私	整合應用及科技於業務流程中，並啟用及支持業務流程	交付提供利益之計劃，需要符合預算、符合要求及質量標準	IT管理資訊的質量	符合內部政策的IT	理解技術和業務且具競爭力及積極的員工	知識、專業能力和業務創新的積極性		
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13		
1 評價、指導及監控		財務				客戶		內部因素					學習和成長		COBIT 2019 映射結果	缺態(%)
EDM01	確保治理框架的設置和維持	P	S	P					S			S			85.66	86%
EDM02	確保收益實現			P		S	S		S	P				S	87.66	88%
EDM03	確保風險優化	S	P					P				S			84.81	85%
EDM04	確保資源優化			S		S	S		S	P			S		89.00	89%
EDM05	確保對利害關係人之參與度				S						P	S			86.39	86%
																87%
2 調整、規劃及組織																
APO01	管理IT管理框架	S	S	P		S		S	S	S	S	P			84.48	84%
APO02	管理策略			S		S	S		P				S	S	86.33	86%
APO03	管理企業架構			S		S	P	S	P						82.51	83%
APO04	管理創新			S			P		S				S	P	84.33	84%
APO05	管理投資組合			P		P	S		S	S					87.33	87%
APO06	管理預算和開支			S	P					P	S				88.17	88%
APO07	管理人力資源			S		S				S			P	P	85.93	86%
APO08	管理關係			S		P	P		S	S			P	P	87.22	87%
APO09	管理服務協議					P			S						82.92	83%
APO10	管理供應商					P	S			S					81.39	81%
APO11	管理質量			S	S	S				P	P				83.46	83%
APO12	管理風險		P					P							83.03	83%
APO13	管理安全	S	S					P							84.48	84%
APO14	管理數據	S	S		S			S			P				80.22	80%
																84%
3 建立、取得及實施																
BAI01	管理方案和項目			P			S		S	P					90.00	90%
BAI02	管理需求定義			S		P	P		S	P			S		83.82	84%
BAI03	管理解決方案識別及建立			S		P	P		S	P					82.48	82%
BAI04	管理可用性和能力					P		S		S					80.00	80%
BAI05	管理組織變革啟用			P		S	S		P	P			S		84.31	84%
BAI06	管理變革		S			S	P		S	S					86.50	87%
BAI07	管理面對變更的接受能力及應對		S				P			S					85.00	85%
BAI08	管理知識			S			S		S	S			P	P	83.61	84%
BAI09	管理資產				P						S				82.25	82%
BAI10	管理配置					S		P							81.39	81%
BAI11	管理方案			P		S	P			P					90.00	90%
																84%
4 交付、服務和支持																
DSS01	管理營運					P			S						81.62	82%
DSS02	管理服務需求及事項		S			P		S							82.64	83%
DSS03	管理問題		S			P		S							80.00	80%
DSS04	管理連續性	S	S			P		P							82.11	82%
DSS05	管理安全服務		P			S		P				S			82.28	82%
DSS06	管理企業流程控制		S			S		S	P	P		S			80.22	80%
																81%
5 監控、評價和評估																
MEA01	監控、評價和評估績效及一致性	S		S		P				S	P	S			80.28	80%
MEA02	監控、評價和評估內部控制系統	S	S		S	S		S		S	S	P			85.54	86%
MEA03	監控、評價和評估是否符合外部要求	P										S			84.21	84%
MEA04	管理保證	S	S		S			S			S	P				
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13		83%
COBIT 2019支援聯合目標的核心治理及管理目標之平均得分		85	83	87	85	83	85	83	83	86	83	85	86	85		

圖 4—COBIT 2019 治理目標及管理目標的映射數據價值之結果

說明：

- 在列中，COBIT 2019 的所有 13 個一致目標
- 在行中，所有 40 個治理與管理目標是藉由訊息技術的治理與管理，按領域分組

COBIT 2019個領域及流程	得分	目標
評價、指導及監控	87%	85%
調整、規劃及組織	84%	90%
建立、取得及實施	84%	95%
交付、服務和支持	81%	90%
監控、評價和評估	84%	90%
	84%	90%

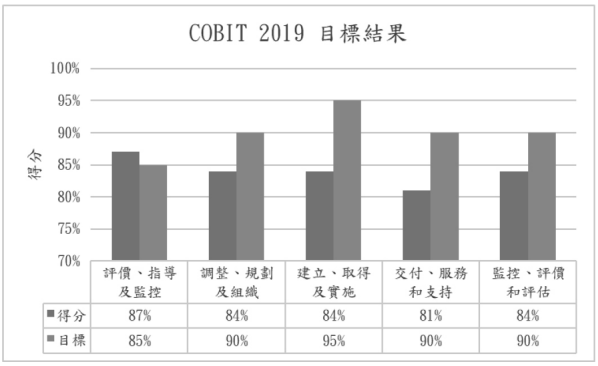


圖 5— 從 BSC 構面解構 COBIT 2019 核心領域的映射數據值的結果

在 COBIT 2019 中，3 個新的管理目標（流程）包括：

- APO 14 管理數據
- BAI 11 管理計畫
- MEA 04 管理確信

這些未出現在 COBIT 5 中，並且影響了圖 2 中的 COBIT 5 下的結果。由於在圖 4 和圖 5 中所示的 COBIT 2019 結果中引入了這 3 個目標，因此圖中沒有 0 分值 與圖 2 結果（ EDM 05 和 APO 08）不同。從圖 5 中的 BSC 表中可以看出，由於引入了這些目標，因此 EDM 的得分更高。 這一結果反映了一個事實，即 EGIT 的 COBIT 2019 框架核心以治理為中心，當被視為策略框架時，COBIT 2019 一旦被採納並適應了組織的文化，便可以幫助組織做出改變。

COBIT 2019架構			將調整目標映射到治理及管理目標														
			具競爭力產品及服務之組合	可控的IT相關業務風險	外部法律及監管之遵從	財務資訊的質量	客服導向的服務文化	企業服務的連續性及可用性	管理資訊的質量	內部業務流程功能優化	企業流程成本優化	員工技能、積極程度及生產力	內部政策的遵從	可管理的數位轉型計劃	產品及業務創新	COBIT 2019支援聯合目標的核心治理及管理目標之平均得分	
			EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13	COBIT 2019 及調整目標之分數	狀態(%)
BSC構面調整目標			財務				客戶		內部因素					學習和成長			
財務	AG01	IT業務的合規性和支援業務遵從外部法律和監控		S	P								S			84.94	85%
	AG02	可控的IT相關業務風險		P				S								83.37	83%
	AG03	從IT推動的投資和服務組合實現利益	S				S			S	S			P		87.06	87%
	AG04	財務資訊相關的技術質量				P			P		P					85.21	85%
																	85%
客戶	AG05	交付與業務需求一致的IT服務	P				S	S		S				S		82.87	83%
	AG06	將商業需求轉換成可實行的解決方案的靈活性	P				S			S				S	S	85.23	85%
																	84%
內部因素	AG07	資訊安全，處理基礎設施、應用程序以及穩私		P				P								83.02	83%
	AG08	整合應用及科技於業務流程中，並啟用及支持業務流程	P				P	S		S		S		P	S	83.34	83%
	AG09	交付提供利益之計劃，需要符合預算、符合要求及質量標準	P				S	P		S	P			P	S	85.91	86%
	AG10	IT管理資訊的質量				P			P		S					82.59	83%
	AG11	符合內部政策的IT		S	P								P			85.15	85%
																	84%
學習與成長	AG12	理解技術和業務且具競爭力及積極的員工					S			S		P				81.62	86%
	AG13	知識、專業能力和業務創新的積極性	P		S					S	S			S	P	82.64	85%
		映射主要支援聯合目標的企業目標	84.53	83.19	85.04	83.90	83.34	84.46	83.90	85.27	85.46	85.59	85.15	85.44	85.27		85%
		企業目標狀態(%)	85%	83%	85%	84%	83%	84%	84%	85%	85%	86%	85%	85%	85%		
			EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13		
		企業目標BSC				84%			84%				85%		85%		

圖 6— 從聯合目標到企業目標 COBIT 2019 映射數據值之結果

根據需要對圖 4 得出的值進行串聯的需求，引入了以標示黃色顯示的觀察結果和更新（ P 和 S），並在圖 6 中使用了這些觀察和更新來定義將在圖 7 和 8 中生成 BSC 的對映。

對映表 - 企業目標與一致性目標如下：AG 08 和 EG 06 應該具有企業的業務連續性管理的輔助支持或關係。用於業務和 I ＆ T 程序管理的 AG 09 和 EG 06 將增強和支持業務連續性管理作為主要功能，或者在 EGIT 中彼此建立了主要關係。

AG 09 和 EG 09 反映了關鍵的關係，應作為基於計劃管理規則並在 EGIT 下表達的

主要功能。如前所述，應將 AG 09 和 EG 09 的這種關係從次要更改為主要。

為了使企業達成 AG 12 和 EG 08 中設定的目標，應該存在次要關係來維持 EGIT 框架的活動。

EG 08 和 EG 09 應該與 AG 13 具有重要的主要關係。員工關係具有策略意義，可以根據 AG 13 中所述的關係來啟動和制定具有知識的創新產品。AG 13 的 P 值的關聯源自 APO 04，APO 07，APO 08 和 BAI 08 的 COBIT 2019 核心管理目標。所有這些都與學習和發展 / 成長（ BSC 觀點 ）有關，並通過人力資源（ HR）功能在組織中進行管理。

映射COBIT 2019的聯合目標BSC	得分	目標
財務面向	85%	85%
客戶面向	84%	90%
內部因素面向	84%	95%
學習與成長面向	85%	90%
	85%	90%

映射COBIT 2019和聯合目標的企業目標BSC	得分	目標
財務面向	84%	85%
客戶面向	84%	90%
內部因素面向	64%	95%
學習與成長面向	85%	90%
	79%	90%

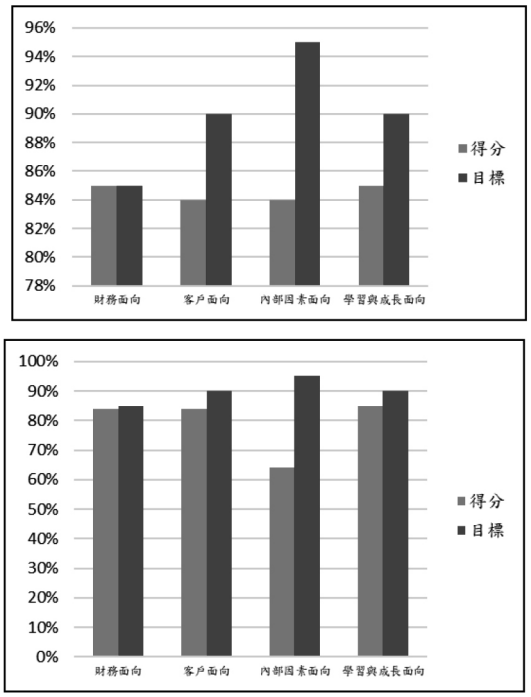


圖 7— 從平衡計分卡角度看 AG 13 和 EG 08 沒有 P 值的影響

對映運用考慮了 EG 08 和 AG 13 的主要功能。該假設基於與 EG 08 相關的企業目標，該目標應該具有主要關係，並且可以通過從 AG 13 獲得的知識來達成。如果未達到 AG 13 和 EG 08 的 P 支持關係值，則得分變為 0，並且此結果會將內部視角 (Internal Perspective) 的分數傾斜為 64%（ 圖 7）而不是 85 %（ 圖 8）。重要的是要注意，EG 08 是 BSC 的內部視角 (Internal Perspective)，而 AG 13 是 BSC 的學習和成長視角 (Learning and Growth Perspective)。

映射COBIT 2019的聯合目標BSC	得分	目標
財務面向	85%	85%
客戶面向	84%	90%
內部因素面向	84%	95%
學習與成長面向	85%	90%
	85%	90%

映射COBIT 2019和聯合目標的企業目標BSC	得分	目標
財務面向	84%	85%
客戶面向	84%	90%
內部因素面向	85%	95%
學習與成長面向	85%	90%
	79%	90%

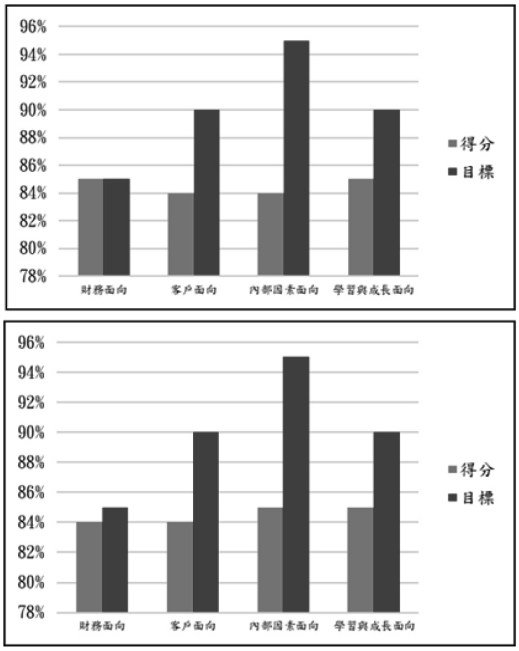


圖 8— 從平衡計分卡角度，為實現聯合目標和企業目標所繪製的 COBIT 2019 資料值之結果

基於BSC的COBIT 2019作為策略績效的衡量標準

BSC 的作者強調了傳統管理系統的缺陷，即傳統的管理系統沒有解決企業的短期戰略與其長期財務目標與之協調。這就是形成 BSC 的 4 個觀點的基礎，這些觀點被描述為財務、顧客、內部因素、學習與發展，以推動企業發展。這些觀點幫助組織教育員工，溝通策略並衡量結果，透過改善財務狀況與回應或客戶成長。

傳統的衡量方法只報告以前的行動或事件，而沒有提供基於策略成果的前進方式或管理者如何在下一階段提高績效的解決方案，記分卡是公司當前和未來成功的基石。

從 BSC 的 4 觀點來看資訊的外部衡量（例如客戶反應和營業收入）和內部衡量（即新產品開發，知識，內部互動和創新）之間取得平衡。績效評估系統（例如平衡計分卡，技能管理工具）用於進一步提煉策略和治理討論以推動企業前進所需的必要數據或資訊。

根據 COBIT 2019 的資訊，使用與 COBIT 2019 治理和管理目標及一致性目標相關的主要價值所做的假設：

- COBIT 2019 目標是達成一致目標的主要支持。
- 這是主要的，當 COBIT 2019 目標和一致目標之間存在重要關係時（與一致目標和企業目標相同）。
- 達成一致目標需要成功地應用和使用許多促成因素。
- 與 3 個主要的企業 I & T 治理重點領域有關係 - 價值交付，風險管理（2 個結果）和資源管理（1 個驅動因素，覆蓋了所有其他重點領域）。

通過從 BSC 觀點的理解以及對主要

支持價值的了解，從業人員可以確定企業及其所在行業面臨嚴重的收入或客戶體驗中斷風險的地方。基於此訊息，可以在這些領域中將構建技能和相關功能作為企業I & T組織內的指針。 AG 13的P值來自APO 04，APO 07，APO 08和 BAI 08的COBIT 2019核心管理目標得分的組合。

沒有EGIT文化，在企業中推動數位化轉型是一個艱難的過程。許多企業擁有合適的技術，但是企業卻難以滿足利害關係人的需求，因為他們保留了不再適合物聯網（ IoT）和數位企業時代工業物聯網（ IIoT）的傳統組織的做法和思維方式。

許多從業人員會同意，許多企業角色現在都需要I & T技能，而大多數I & T角色都需要非技術技能 - 從理解人類行為（即心理學，社會科學 ）到設計思維，敏捷團隊合作，甚至人類與AI / 機器學習之間的交互（ ML）。這些有助於I & T為未來進行創新。解決此問題的方法是採用EGIT框架（ COBIT 2019）進行交互 / 對映，以調查企業及其行業面臨嚴重的收入或客戶體驗中斷風險的地方，然後開始在這些領域內建立技能和相關能力企業I & T組織。它還有助於重新審視企業的數位企業轉型路線圖。

利害關係人還必須對照企業領導者的野心評估當前路線圖的速度和有效性的現實情況。如果存在阻礙進步的差距，則人力資源和C級人員應參與計劃數位敏捷性計劃，以發展未來的勞動力。數位敏捷企業超越了技術知識、技能和思想的傳統界限。正如一位作者所指出的那樣，“擾亂要求（在競爭中 ）創造新的基礎，通常與任何現有範式平行”。

結論

COBIT 2019解決了這些缺點（即採用治理框架，面臨收入中斷的風險，缺乏路線圖 ），並使該框架更易於適應並被企業用作EGIT的總體框架。COBIT 2019幫助建立關係（聯繫戰略團隊 ）; 與執行發起人一起確定外部策略機會、對於從業者、管理人員、數據和技術。從通過ISO/IEC 27001到COBIT 5到COBIT 2019的對映獲得願景和戰略驅動力分數。通過將COBIT 2019治理和管理目標對映到一致性目標然後再對映到企業目標的結果表明，如果使用正確，則策略可以此對映工作有助於從COBIT 2019框架中得出結論。策略學習包括收集反饋，測試治理策略所基於的假設並進行必要的調整，這是該對映活動幫助從COBIT 2019框架中得出的。一致性和企業目標分數構成了組織制定行動計劃的基礎，以解決ISO / IEC 27001控制目標的輸入項並確定計劃的發展 / 糾正路線圖需要解決的問題，作為組織的一部分企業策略。可以得出結論，在策略規劃中使用COBIT 2019可以得成目標是有效的，採用戰術行動來實施該策略對企業運營至關重要。

克里斯托弗·C· 阿諾魯 (Christopher C. Anoruo), CRISC, CISM, CGEIT

是一家網絡安全公司TRAFTEC Ltd的首席執行官。他曾是KATEC Consulting Ltd.的技術和運營總監的執行董事。他還曾在西非的電信和銀行業擔任過多個職位。在與他人共同創立KATEC Consulting Ltd之前，他是IBM Global Business Services的資訊安全顧問。 Anoruo已經為ISACA認

證的資訊安全經理（ CISM），風險和資訊系統控制（ CRISC）認證以及企業 IT 治理（ CGEIT）考試認證做出了貢獻。他還參加了 ISACA 認證項目，並且自 2005 年以來一直是 ISACA 測試增強委員會的成員，負責設置考試題和複審考試手冊。

原文出處

1. https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy

透過COBIT 2019框架指引達成企業的數位轉型

Achieving Digital Business Transformation Using COBIT 2019

作者:

Oluwaseyi Ojo, Ph.D.

COBIT 5 Certified Assessor, ITBMC

譯者:

黃誌緯

安永聯合會計師事務所 資深經理

mail: Danny.Huang@tw.ey.com

陳冠穎

安永聯合會計師事務所 資深顧問

mail: Joy.KY.Chen@tw.ey.com

羅珊

安永聯合會計師事務所 資深顧問

mail: Iris.Lo@tw.ey.com

黃晨瑀

安永聯合會計師事務所 資深顧問

mail: Chaney.Huang@tw.ey.com

摘 要

隨著應用科技的快速發展，數位轉型將是企業迫在眉間的議題。數位轉型是一

個借助數位科技或是將數位科技和商業整合的過程，本文說明數位轉型對企業的影響，並描述如何使用 COBIT 2019 框架進行規劃，協助企業有效率及妥善地進行數位轉型。

關鍵字 : COBIT 2019、數位轉型、企業思維、ISO/IEC 38500

正文

當前經濟的數位轉型不再是一種選擇，而是企業必須立即採取的行動。執行數位專案經驗不足及小幅度的策略調整，無法為轉型帶來本質上的改變，這意味著許多企業主對於數位轉型有認知上的錯誤。企業主在帶領組織邁向真正的數位轉型前，必須體認到小幅度的調整及徹底的轉型，有著根本上的差異。

85% 的企業決策者表示，他們必須在 2 年內於數位轉型上取得重大進展，否則將落後競爭對手並遭受財物損失。[1]

56% 的企業執行長 (CEO) 表示數位轉型帶來更多的收益和利潤。[2]

即使數位化和轉型的必要性無庸置疑，領導者仍經常問「我們該如何做到轉型？該針對什麼進行轉型？」COBIT 2019 框架能回答這些問題，並協助領導者排除障礙以及維持策略性的數位企業思維轉型。

壹、什麼是企業數位轉型？

數位轉型並不是要企業組織使用特定的新科技；恰恰相反地，它涉及對新科技的了解，以及如何藉由新科技提供顧客、合作夥伴、利害關係人以及員工價值和全新的體驗。數位轉型關乎的是企業組織能否快速反應，以及成功利用新科技和方法在現今和未來蓬勃發展。

「當蛇褪去外皮，這意味著改變；當毛毛蟲化成蝴蝶，這代表著轉型。」[3]簡單來說，改變著重的是改善過去或當前的狀態，轉型則更具有前瞻性，並會改變或創造未來。即使改變是件好事，但它充其量只是改善舊有的商業模式，當企業領導者、理事會、行政主管和資深經理了解改變和轉型的差別前，企業組織在執行層面上所做的策略調整，會使他們持續陷入轉型的幻覺，這將導致危險的後果。數位轉型是一個借助數位科技或是將數位科技和商業整合的過程，而這樣的轉型能影響科技、文化、工作環境以及其他更多面向。舉例來說，Uber 借助科技的力量，讓計程車產業完成數位轉型。其他案例還包括旅館業的 Airbnb 以及通訊產業的 Skype 和 WhatsApp。

一、對企業數位轉型的誤解

關於企業數位轉型仍存有許多誤解，如以下幾個例子：

(一) 企業能以舊有的思維和商業模式達成數位轉型

這是最讓人感到匪夷所思的一項誤解了，「轉型」這個詞本身就暗示了企業的流程或是產品已不再是原來的樣貌。商業模式指的

是組織如何賺錢和獲利的計畫；商業思維則是組織在梳理出轉型策略後，於實務中予以實踐。新的商業思維意味著 (策略性) 以新的方式創造不同的事物，透過新的思維模式，找出潛在市場及市場中可利用的機會；它還能敏銳地察覺潛在的勁敵，及應對他們的方式。這一套開放的思維模式，能快速適應變革的環境以及組織從未碰過的挑戰。在現今的數位經濟下，想保有競爭力的組織必須將數位化納入其組織的核心商業模式之中，換句話說，組織必須有一套數位化的商業模式以及新的商業思維才能蓬勃發展。舉例來說，傳統計程車業已經很難在低價的同時，提供高水準的服務，然而多數的計程車業者仍相信舊有的商業模式是可行的，沒有人預見 Uber 帶來全新的思維和商業模式。Uber 的新商業模式提供一個媒合平台，讓有汽車的民眾透過這平台載送乘客來賺錢，和傳統計程車業相比，Uber 司機因為可以彈性的選擇工作時間，較容易從中獲得更高的利潤。這樣的新商業模式能更機動地整合線上的司機，分配載送的範圍，讓乘客可以透過行動裝置指定司機載送，因此轉型必須透過改變思維模式和商業模式來實現。

(二) 組織執行企業數位商業轉型計畫需要大量的預算

預算有限的組織仍可以投資數位轉型。許多案例顯示，大筆預算的企業數位轉型計畫往往都會失敗，然而在關鍵的領域投資小筆預算不僅會轉型成功而且還能延續。英國廣播公司（BBC）就是一個投資了大筆預算但最終失敗的案例。在 2013 年，BBC 取消了數位媒體計畫 (DMI)，當初該計畫是為了因應數位化趨勢，且計畫斥資 1. 624 億美元。[4]

(三) 在組織的每個人都應了解企業數位轉型

根據過去經驗顯示，企業間對數位轉型計畫的重點、規模和目的理解各不相同，而組織中的每個人可能對企業數位轉型的重點、規模和目的有不同的定義，這些差異就是造成計畫失敗的主要原因之一，所以組織領導人應明確定義並解決理解上的差異。

(四) 企業領導者通常會堅持己見且固守在舊有的商業模式

成為產業龍頭，已不能保證可以在現今的全球市場長久的成功。我們應謹記：「過去的成功無法保證未來的成就」[5]，當組織在全球激烈競爭的狀況下，卻未能走出自己的舒適圈而轉型時，他們可能會錯失機會，且可能將面臨被市場淘汰的下場。任何組織都無法倖免於破壞，Motorola、Kodak、Nokia 和 Blackberry 都因組織領導人故步自封，導致這些

企業所被熟知的許多產品幾乎都已被市場淘汰。

貳、為什麼要進行企業數位轉型？

大多數的領導者都認知數位商業轉型的好處，但許多組織都尚未徹底執行，有些企業執行了非策略性的數位化改變，但相對卻少有企業策略性的執行數位轉型。

從「為什麼要轉型？」為出發點，許多企業領導者知道他們需要轉型的原因，但通常他們不知道該如何執行，也沒有採取行動。

參、企業數位轉型的痛點和觸發事件

組織在初步規劃數位轉型計畫時必須注意轉型的痛點和觸發事件。若不慎重考量和解決這些因素，可能會導致轉型計畫的失敗：

一、組織文化

文化通常是成功實施數位轉型計劃時最困難的挑戰之一，領導者需透過協調並引領邁向數位轉型之路以成功改變組織文化。

二、管理層的抗拒

管理階層中的某些成員可能不認同組織需進行數位轉型的必要性，或將轉型視為一種威脅，所以執行長必須與管理階層密切地合作，直到獲得他們完全的支持，這樣才能讓管理階層準備好應對組織中更廣泛的文化挑戰。

三、員工反對（即員工恐懼或抗拒）

員工可能會對轉型抱持懷疑的態度，並擔心數位轉型可能會威脅到他們的工作，員工通常會有意識或無意識地抗拒轉型。此外，建立企業文化的目的是為了維持組織的現狀。大多數員工在過去都曾目睹過失敗的專案和計畫，所以他們可能對數位轉型持有懷疑態度並不令人驚訝。

四、缺乏領導數位轉型開端的專業知識

當沒有企業數位轉型的技術人才帶領轉型開端時，就會發生這種情況。

五、缺乏數位化策略

若未將數位化與商業策略整合，數位轉型必然會面臨失敗。

六、企業數位轉型策略未與企業目標一致

數位轉型往往因為目標從一開始就不明確，導致無法充分發揮其轉型效益，即使數位轉型目標清晰，但與企業目標不符時，轉型終將注定失敗。

七、缺乏創新的商業環境

創新是轉型的驅動力，營造鼓勵創新，並有效交流、參與、合作的環境對於成功推動數位轉型是極其重要。

八、缺乏轉型的願景、策略及規劃

領導者需具體建立組織轉型願景，否則，組織將因缺乏明確目標而停滯不前。資深經理人有責任向全組織澄清和傳達數位轉型的願景及策略。

九、轉型和改變的模糊地帶

組織領導者需清楚定義出改變和轉型的差別，否則可能導致組織誤以為在轉型，但事實上僅是在改善舊有的商業模式。

十、缺乏了解顧客需求

隨著顧客期望的改變，組織必須要找出能與競爭者做出區隔的領域。數位經濟競爭中的勝負，將取決於組織對其客戶期望的了解，以及組織提供卓越顧客體驗的能力。

十一、缺乏企業數位轉型的思維

領導者必須具備正確的思維及改變原有的思考模式，才能有效應對數位經濟所帶來的挑戰。

肆、企業數位轉型的驅動和落實

反之，有些因素能驅動和實現數位轉型，並確保轉型成功。組織在執行數位轉型時須將這些因素納入考量。

一、創新 / 創新管理

創新是數位轉型的成功關鍵，領導者必須了解，在缺乏適當的創新能力狀況下，企業可能只是單純使用新科技執行舊有業務，其效果既不創新也不算轉型。

二、競爭力

數位化幫助大型企業及大中小型組織展現極大的潛力，使已落實數位經濟的企業擁有競爭優勢。

三、成長

數位轉型是達成數位經濟時代下企業成長和成功的關鍵。

四、顧客洞察力和期望

一旦企業無法滿足顧客不斷增長的期望時，顧客將減少購買與期待不符的產品。

五、價值主張

當顧客有更好的數位導向價值主張時，顧客將會失去原有的忠誠度，並選擇更好的產品。

六、組織數據

詮釋組織內部及外部的資料是大幅改變組織績效的關鍵，蒐集數據並不困難，但詮釋數據資料卻是許多組織面臨的難題，正確解讀數據，才能完全發揮出其價值。

七、轉型管理

領導者需要確定自己具備足夠執行數位轉型管理的能力，否則將在執行時遇上許多挑戰。

企業數位轉型有多種形態，而每個組織都有獨特的需求和優先順序，不論需求為何，一個正確的框架能協助串聯業務部門和 IT 部門內的所有相關利益者，共同決定該轉型事務及方式。這會進而讓組織內部一致，並提供探索轉型事物的共同語言，當組織所有人取得轉型的共識後，它們將依照藍圖共同完成目標並熟悉整個程序，使用共通的架構並不會侷限創新，它反而能讓更多人換位思考，發現更多的機會。

採用共通的框架能避免人做出未經計劃的行動、使用前衛卻不恰當的科技、或只狹隘的著重在銷售。組織不應該受其他因素影響而鼓勵孤立奮戰或和隨意改變轉型策略及

計畫的優先順序。COBIT 2019 提供適當的企業數位轉型目的、目標和方法。

伍、如何數位化的轉型：COBIT 2019

針對數位轉型，資訊科技在協助、維持及公司成長方面扮演了非常重要的角色。

COBIT 框架提供了全球通行的準則、措施、工具及模型以協助提升對企業 IT 部門的信賴及價值。

COBIT 明確區別治理和管理的目標，並與國際標準化組織 (ISO)、國際電工委員會 (IEC) 標準 ISO/IEC 38500 標準接軌，COBIT 以評估、指導及監督的角度實踐治理目標，並以規劃、構建、執行和監督活動角度實踐管理目標，協助企業達成目標的成功要素。[6]

值得一提的是 COBIT 是一個指導準則，您應該針對其準則開發適合治理及管理資訊科技的解決方法。

一、步驟一，建立由資深管理層及高階主管領導的數位轉型團隊 / 委員會，轉型將對企業帶來重大的影響，所以應讓適任的管理層參與，以確保沒有任何相關人員被遺漏。教育及調整領導心態也相當重要，組織可以透過會議或專題研討，將教學重點放在數位轉型的 WHAT(做什麼)、WHY(為何做) 及 HOW(如何做)，幫助每個組織每位成員了解轉型的必要及數位破壞可能會帶來的風險，轉型成功的關鍵不單仰賴科技，更需仰賴團隊或委員會對於業務需求、驅動因素及風險的充分了解。

二、步驟二，選擇適合的設計因素，例如：企業策略、企業目標、風險概況、IT 角色、技術採用策略及企業規模。

三、步驟三，選擇適合的重點領域，例如：數位轉型或網路安全。

四、步驟四，企業可利用目標層級分派，透過分配目標到各執行人員，將利害關係人的需求轉化為可行的策略，進而根據目標的優先順序選擇適合的治理及管理目標。

五、步驟五，設計量身訂製的治理系統。

六、步驟六，根據第四步所選擇的治理及管理目標來確定其優先順序。

七、步驟七，選擇適用於治理系統的組成要素。

八、步驟八，建立全面的轉型計畫，以確保所有優先的治理及管理目標都有納入考量，大多數企業發現有時目標的增減，造成最終導致成果不符利害關係人的期待。為幫助成員達成共識，企業應記錄及傳達數位轉型的定義。

九、步驟九，雖然做好轉型的準備相當重要，但卻有許多組織往往缺乏充分準備。

當前的轉型準備程度需根據以下準備度要素評估：

(一) 組織文化
(二) 企業治理
(三) 創新能力
(四) 數位能力
(五) 轉型管理能力

(六) 組織架構

(七) 任何會阻礙或阻擋轉型工作的挑戰或障礙

採用能力成熟度級別矩陣來協助確認每個準備度要素在成熟度級別上的位置，依據現況到未來可能面臨的轉型挑戰，商定各階段應具備的準備度要素。利害關係人應根據實際情況及成熟度級別來執行轉型，否則可能會發生轉型風險。

十、步驟十，利害關係人透過實施及管理轉型開始執行或部屬轉型策略。

陸、結論

遵照以下步驟並使用 COBIT 2019 框架來找出適當的數位轉型目的、目標及方法，可以創造下列優勢：

一、達成策略目標並實現企業效益

二、透過有效使用技術優化營運

三、維護準確且有品質的資訊以用於指導企業決策

四、優化 IT 服務及節省技術成本

規劃數位轉型策略是一個持續的過程，數位轉型將對企業各方面帶來重大的變革，因此必須於各方面包括適當治理、企業思維、商業模式、能力及文化做好妥善準備，企業才能邁向數位轉型成功。

注釋

1. Morgan, B.; “40 Stats on Digital Transformation and Customer Experience,” Forbes, 13 May 2019
2. DeNisco Rayome, A.; “Report: 56% of CEOs Say Digital Transformation Has Increased Profits,” TechRepublic, 24 April 2017
3. Llewellyn, R.; “What Is Digital Transformation?” CXO Transform, 1 January 2016.
4. National Audit Office, British Broadcasting Corporation Digital Media Initiative, United Kingdom, 2014
5. Goldsmith, M.; What Got You Here Won't Get You There: How Successful People Become Even More Successful, Writers of the Roundtable Press, USA, 2011
6. ISACA, COBIT 2019 Framework: Introduction and Methodology, USA, 2018

文獻原文

1. Author, Oluwaseyi Ojo (2019). Achieving Digital Business Transformation Using COBIT 2019., COBIT Focus.

School Accounting Education in Japan

—In Relation to Economic Development of the Country

Yoko, SUGA
CEO, International Business Alliance Inc.
Tokyo, JAPAN, yokosuga0806@gmail.com
Toshifumi TAKADA
Professor, National Chung Cheng University
Chiayi, TAIWAN, ttakada0830@gmail.com

I. INTRODUCTION

This is an introductory article to Japanese accounting education history in relation to country's economic development. The authors (Yoko SUGA and Toshifumi TAKADA) were engaged in the education of international education program in accounting (IGSAP)[1] since 2015. We understand that accounting has contributed to the development of the Japanese economy in these 150 years. Since 1868 when modern Japan started, there have been three stages of accounting contributions to the development of the Japanese economy. It is our objective to trace how accounting has contributed to the development of the Japanese economy and how higher university played its role in accounting education in each stage.

II. EDUCATION OF BOOK-KEEPING: The 1st stage 1868-1945

2- 1. Outline of this stage

The 1 st stage of accounting contribution is the education of bookkeeping. One of the main players of this stage is Yukichi Fukuzawa (1835- 1901, a founder of Keio University). Yukichi Fukuzawa was an officer (Samurai)[2] of the Tokugawa government (1603- 1868). After the inception of modern Japan in 1868 he started a school that later became Keio University. When he visited the US in 1860, he

understood that bookkeeping in the US was different from the Japanese method. After having returned to Japan he got a textbook, Bryant & Stratton's Common School Book-keeping, widely used at the business schools in the US. He translated the textbook into Japanese and he used that book for education at Keio Gijyuku and at a bookkeeping school. Graduates of Keio Gijyuku and that private school (Keio Gijyuku has become one of the established private universities in Japan, Keio University) were educated in bookkeeping and they worked in the accounting departments of many companies. Bookkeeping is a technique of accounting and modern companies could make informed decisions by the financial statements prepared by bookkeeping.

2- 2. Textbook of this stage

Fukuzawa knew single entry bookkeeping widely used by Japanese merchants until the 18th century. When he visited the US, he noticed the difference between single entry bookkeeping and double entry bookkeeping. As we know, the double entry bookkeeping procedure begins from journalizing a transaction into debtor and creditor, making journal and ledger, and preparing financial statements. Merchants and manufacturers could know the companies' profit or loss and financial conditions through financial statements.

Fukuzawa purchased a most popular textbook titled "Bryant & Stratton's Common School Book-keeping [3)] " in 1871 and translated it into Japanese. He told the advantage of using this book in a school as

(1) Scholars are poor as they don't know practical knowledge, but this book is practical.

(2) Single entry bookkeeping needs lots of time to know profit or loss but this book will solve this problem

(3) Everyone high and low can study bookkeeping by this book.

(4) All occupations are business to earn money. There are no differences between occupations. Learning bookkeeping is the basics of business.

The content of the textbook is as follows.

Table 3. Contents of Bryant & Stratton's Common School Book-keeping in 1871

Part I.	SINGLE ENTRY
INTRODUCTION TO PART I.	
SET I.	Introductory-Showing the use of the Books.
SET II.	Retail Dry Goods. (Prosperous.)
SET III.	Wholesale Dry Goods. (Adverse.)
SET IV.	Furniture and Cabinet Business. (Prosperous.)
PART II.	DOUBLE ENTRY
INTRODUCTION TO PART II.	
SET I.	Produce Business. (Introductory.)
SET II.	Grocery Business. (Prosperous.)
SET III.	Wholesale Dry Goods. (Adverse.)
SET IV.	Gentlemen's Furnishing Business. (Prosperous.)
APPENDIX.	

2- 3. Place of bookkeeping education

Fukuzawa taught bookkeeping at his school. In 1890, Keio Gijyuku started university education but before that in 1880 he had a professional school for bookkeeping education. We can understand that his education played an important role in the development of modern Japanese economy as the graduates of his school were employed by companies and did accounting jobs. Companies in the evolving age of Japan could use the financial statements. Without accounting they could not navigate their companies in the right direction.

III.PROFESSION AND ACCOUNTING REPORTING: The 2nd stage 1946-2000

3- 1. Outline of this stage

After World War II, the Japanese government decided to introduce Certified Public Accountants (CPA) from the US. Until then, professional accountants called Keirishi existed but the Japanese government changed Keirishi (Japanese professional Accountants)[4] to CPA. CPA is responsible for auditing of financial statements disclosed to investors in the stock Market[5]. The entire economic system was completely destroyed by World War II, so companies started from zero in 1945 and they needed investment from the US. Investors required reliable accounting reporting and CPAs as auditors of financial statements

were needed by investors. At the same time, the Japanese government introduced another professional accountant system called Tax Accountant)[6]. These dual professional accountants contributed to the recovery of the Japanese economy. Education for professional accountants was made at a few large private universities and professional schools of national universities. The Japanese economy recovered in the 1960s and experienced a big success in the 1980s. It was a real miracle. Professional accountants played an important role at this stage and university education contributed to them.

3- 2. Education for Certified Public Accountants

The Ministry of Finance was also responsible for the qualification examination called CPA Examination. It was very difficult to pass but fortunately, after World War II, as the Japanese military was dissolved, many excellent young people sat the examination. They sat CPA Examination and they studied the subjects of the Examination. The accounting subjects were Bookkeeping, Accounting, Cost Accounting, and Auditing. They studied these subjects at a few universities such as Chuo University, Waseda University and Keio Gijyuku University. These universities educated accounting and auditing to such people. The number of people who passed the CPA Examination and registered at the Japanese Institute of Certified Public Accountants (JICP) was increasing year by year as shown in the table as follows.

Table 4-1. Number of CPAs registered at JICPA

Year	1950	1960	1970	1980	1990	2000	2010	2020
Number	392	2, 172	5, 134	8, 357	11, 401	16, 656	27, 792	39, 195

source: The Japanese Institute of Certified Public Accountants

＊1 Included candidates, foreign CPAs, audit firms

＊2 Candidates are person who passed CPA Examination

The number of CPAs increased rapidly several years ago and the total number of CPAs registered reached 39, 000 in 2020. The role of education of university has been substituted by a few preparatory schools in recent years as passing CPA Examination has become too difficult and university education has not coped with it. This means that the university education for professional accountants doesn't function at all for the students sitting the CPA Examination. This became a big problem to be solved.

3- 3. Education for Tax Accountants

The manufacturing industry developed both after 1868 and after 1945. There are about

5, 000, 000 business corporations in Japan and almost of them are SMEs. The number of listed companies is just 3, 500 (0. 7%) and 99. 3% are SMEs. Financial statements of SMEs are not required to be audited and disclosed. SMEs have contract with TA offices and not with CPA firms. The main job of TA offices for SMEs is to prepare the tax return documents and report them to the National Tax Agency (NTA).Only TA is permitted to report the tax return to NTA on behalf of clients.

Many SMEs outsource accounting jobs to the TA offices. As they are professional accountants, they know everything about corporate tax and other taxes. TA offices can do tax planning for clients. They also make advisory services about minimizing tax payments. It is not an evasion of tax. TA is closely related to the NTA. After the Tax Accountant Law was amended in 1951, TA has become recognized as a professional accountant.

TA qualification is more complicated than CPA qualification as it admits a few by passes. One of them is giving qualification to the retired person of NTA. And Lawyers and CPAs are also by passes. Such qualified people can make registration at the Association of TA without any examinations and they can do job as TA. As a result of this, the total number of TAs registered is much more than CPAs. The following table shows this.

Table 4-2. Number of Tax Accountants registered at Tax Accountant Association

Year	1951	1960	1970	1980	1990	2000	2010	2020
Number	3, 944	10, 888	24, 024	40, 535	57, 073	65, 144	72, 039	78, 617

source: Japan Federation of Certified Tax Accountants' Association

The number of people sitting the TA qualification examination was not so many compared with CPA Examination because of a few bypasses to get the qualification. There are five subjects of the examination and it is not necessary to pass five subjects at once. Instead, it is possible to pass each subject one by one in each year. The education for them depended on the prep schools and not universities. Mainstream for TA qualification was flow from the NTA retired people, and they need not sit the TA examination.

Main stream of TA qualification was alumni people of the National Tax Bureau (NTB). As a result of this, education for them was done by the school of NTB. Main subjects taught there were income tax, corporate income tax, indirect tax, heritance tax, etc.

IV.REQUIREMENT OF PROFESSIONAL ETHICS AND CAAT:The 3rd stage 2001-now

4- 1. Outline of this stage

After the Enron scandal in 2001, many accounting scandals occurred both in the US and in Japan. One of the authors, Toshifumi Takada, was a founder of the accounting school of Tohoku University and he was also a founder of the Association of Accounting Schools in Japan. He visited key persons of the International Accounting Education Standards Board (IAESB) of the International Federation of Accountants (IFAC) and had a few seminars in Tokyo on the IFAC's education standards. He recognized the importance of the necessity of the education on professional ethics. The Report on the Core Curricula of accounting schools influenced all the accounting schools' curricula and they started education on professional ethics. The 3rd objective of this paper is focused on university education of professional ethics.

4- 2. Education of Accounting Ethics

The Japan Association of Graduate Schools for Professional Accountancy (Association of Accounting Schools) organized a committee on core curriculum for accounting schools in 2010. Accounting Schools started in 2005 and each school had its own curriculum. The Ministry of Education, Culture, Sports, Science and Technology (Ministry of Education) thought that it was necessary for professional schools to have standards, core curriculum. They supported the budget to do a field survey of core curriculum. The Association of Accounting Schools got the budget and organized a committee of core curriculum.

This committee disclosed a report, "Report of the Committee of Core Curriculum" in 2010[7]. In this report, the committee recognized the importance of subjects related to accounting (bookkeeping, cost accounting, financial accounting, management accounting and auditing). In addition, it recommended four courses as core subjects to be added: accounting professional ethics, International Financial Reporting Standards, computerized assisted audit aided techniques, and internship.

4- 3. Education of CAAT

Report of the Committee of Core Curriculum, Association of Accounting Schools also requires a course of Computer Assisted Auditing Techniques (hereafter CAAT or IT Audit). 60 licenses of ACL[8] are used at 3 accounting schools for the education of CAAT. The objective and outline of this course is shown in the Report as follows.

The objective: Using information technology (IT) is indispensable in accounting and auditing practice. This condition requires accounting professionals to be equipped with the higher knowledge of IT and its application abilities. The International Federation of Accountants (IFAC) published the draft on

International Education Practice Statement "Information Technology for Professional Accountants. IFAC required the professional accountants to have higher knowledge of IT.

In this course, students study IT knowledge and practice focusing on Computer Assisted Audit Techniques (CAAT).CAAT has now become one of the important audit procedures as the client companies use IT. Until recently, audit standards require sampling procedure but using CAAT, auditors can execute a detailed audit; they audit all the transactions and evidential matters by using CAAT. ACL (widely used as a CAAT software) is used in this course.

Outline:

1- 3: Class: Basics of CAAT

4- 5: ACL commands

6- 15: ACL programming for major topics

Profession and accounting professionals facing accounting fraud must change the old-fashioned audit procedure from sampling method to detailed method. The regulatory body, stock market, stakeholders require the auditor to detect accounting fraud. Auditors must satisfy this requirement. CAAT is one of the key factors to complete this difficult mission.

V. RELATION OF ACCOUNTING TO ECONOMIC DEVELOPMENT

Accounting has been one of the key factors for the development of the modern Japanese economic development after 1868. Accounting in Japan has played a pilot role for the business organizations. Its impact was not only for the business but for the Japanese government. With accounting reporting, the Japanese government could collect tax and it could keep sustainability. Accounting contributed to the economic development at the time of 3 big changes in Japan.

5- 1. Informed decision based on financial statements

DuPont was famous for its chart room in the 19th century. This chart room exhibited many charts of DuPont's business results and financial conditions. The CEO and other top executives used this room for their decision making. They had to recognize the realities of the company before their decision making. This is still true even today for small, medium and large companies. We know many CEOs in Japanese companies have daily sales reports and monthly, quarterly and yearly financial statements. They have meetings using these reports and financial statements.

This became possible in Japanese big companies and banks from the 1880s as they could have accounting departments where financial statements were prepared using double entry bookkeeping and cost accounting. Double entry bookkeeping is the fundamental technique to make financial statements. By journalizing all transactions, profit and loss statement and balance sheet can be made almost automatically. At the age of Edo era until 1868, merchants had single entry

bookkeeping. Merchants could recognize just a few important assets written in a book by single entry bookkeeping at the age of Edo era in the 17 th to 19 th century. Double entry bookkeeping could show the whole picture of a company. It was a revolutionary change.

Translating a textbook of bookkeeping and educating bookkeeping at the beginning of modern Japan by Yukichi Fukuzawa made it possible for the Japanese economy to change from agriculture to manufacturing industry. It is estimated that 95% of GDP was produced by agriculture before 1868 but the industrial structure changed rapidly between 1868 and 1945.

Manufacturing companies needed profit calculation for business decisions. In addition, they must have invested money in long lived fixed assets such as plants, machines, and equipment. On the other hand, farmers could know the amount of rice and vegetables harvested in a year without double entry bookkeeping. They did not need to know the profit number. Japan was very fortunate as Yukichi Fukuzawa introduced bookkeeping at the beginning of industrialization. CEOs and top executives could make informed decisions in their business by financial statements prepared by double entry bookkeeping. Accounting function for informed decision was possible by introducing and educating bookkeeping starting in 1986 until 1945.

5- 2. Transparency for stakeholders

Nobel Prize scholar Kenneth Arrow advocated that democracy was impossible to realize. Its proof was shown in his famous book titled “Social Value and Individual Choice”. We know that theory and practice is different, and he didn't know bookkeeping and accounting. In the accounting context we must discuss democracy in the real world. In the stock market, listed companies are required to disclose their real profit or loss and financial condition. “Real” means that financial statements must be audited by professional accountants. This is called transparency.

Bookkeeping refers to the processing of daily transactions data. Accounting refers to the reporting of results of processing to the people who need the information in order to make informed decisions. CEOs and stakeholders can understand the listed companies, and such companies are transparent to everyone both inside and outside the companies.

Professional accountants had a heavy duty of auditing the disclosed financial statements. It was a legal requirement. The 1933 Securities Act and the 1934 Securities and Exchange Act required auditing by CPA, and CPA has become a watchdog for the stock market. Bookkeeping and accounting were conceptually divided since then into two functions: processing and reporting. Professional accountants accepted an auditing function. As a result of this, CPA qualification became social status. Only qualified CPA could do audit of listed company.

CPA Examination was held by the Ministry of Finance, Japanese government. The Japanese government introduced financial audit by CPA from the US in the 1950s. This means that accounting reporting for stakeholders started and that the significance of accounting reporting was recognized in Japan. Universities accepted the education for the candidates of CPA sitting CPA Examination.

On the other hand, Tax Accountants (TAs) played an important role for SMEs. TAs had a contract with SMEs about processing daily transaction data, preparing monthly and yearly financial statements, and reporting tax return documents (yearly financial statements) to the National Tax Agency (NTA). Almost all the SMEs did this outsourcing accounting jobs to the TA office. Tax return documents are confidential to the public but NTA and the Japanese government know everything about SMEs through the documents. This helps the Japanese government make necessary economic policy.

Tax return reporting was possible as almost all the SMEs had contracts with the TA office. The invoices of daily transactions were forwarded to the TA office and they made journal, ledger and financial statements for SMEs. SME owners (CEOs) received financial statements from the TA office monthly and yearly and they understood the profit or loss and financial condition of their companies.

And more important, the Japanese government could levy corporate income tax and employee income tax by the reported tax returns. Modern countries depend on the income tax. Japan made it possible after 1950s. Professional accountants, CPAs and TAs, were absolutely essential for Japan. Financial statements audited by CPAs and prepared by TAs are correct and reliable. Professional accountants have played an important role in this.

5- 3. Pilot for all the companies

The third is the pilot (steering or navigating) function for companies. CEOs are the leaders of companies. Their decisions must be based on real-time and correct information. Accounting can provide such information for CEOs and executives. Besides accounting can produce many kinds of information including hourly, daily, weekly, monthly, quarterly and yearly financial statements.

Convenience stores are said to be a successful business model in Japan by using accounting information effectively and efficiently. Point of Sales (POS) systems produce sales data and Electric Order Systems (EOS) produce inventory data. These systems are connected with headquarter office, makers, vendors, logistic companies in real time by Internet.

Computer Integrated Manufacturing (CIM), Material Requirement Planning (MRP) and Just In Time (JIT) and Internet of Things (IoT) are being widely used by many advanced companies in Japan. Accounting is supplying information for all these systems.

CEOs need accounting information

because it can navigate them. We know that many SMEs and large companies have daily, weekly and monthly meetings with employees, managers and directors. Successful business models show that accounting plays a pilot function to navigate them.

VI. CONCLUSION

(1) The 1st stage: Yukichi Fukuzawa was a key person at this stage. He translated a bookkeeping textbook into Japanese and he taught bookkeeping at a private school which developed to Keio Gijyuku University. Double entry bookkeeping is a basic technical structure of calculating profit or loss and financial conditions of companies. Without bookkeeping, market economy couldn't survive. The modernization of Japan couldn't be achieved without Fukuzawa and his school.

(2) The 2nd stage: World War II destroyed all the cities and economies in Japan. Japan had to start from zero. The Japanese government learned professional accounting from the US and introduced CPAs. At the same time, the Shoup Mission visited Japan twice and reported about Japanese taxation structure. It included Tax Accountants (TAs). CPA played its role as an auditor for listed companies; TA played its role as an accountant for SMEs. Large private universities (Chuo, Waseda, Keio Gijyuku) contributed education for professional accountants.

(3) The 3rd stage: At the beginning of the 21st century, a big accounting scandal happened. The governments that have a stock market faced a difficult issue to prevent accounting crime. The Enron scandal was just a beginning. Unfortunately, in Japan, big accounting scandals Kanebo (2005), Olympus (2010) and Toshiba (2015) occurred after Enron. Everyone concerned recognized the importance and necessity of the education of accounting professional ethics. Accounting schools played the role of education for ethics.

Accounting is a key factor for the development of an economy. In Japan, universities have provided accounting education for 150 years. We demonstrated the three stages of Japanese accounting education and university.

FOOTNOTES

1. IGSAP is International Graduate School of Accounting Policy launched in 2015 by Tohoku University. This is a professional school and graduates can take double MA

degrees from Tohoku University and their home institution. IGSAP is supported financially by the Ministry of Education. Support will end in 2021 and IGSAP will be closed then.

2. Samurai was a class of people governing Japan since the 12 th century. Before that, the Emperor occupied the position of ruler but Yoritomo Minamoto established Samurai government in 1192 and he was nominated as a leader of Japan from the Emperor. After 1192, Samurai government continued until 1868.
3. Old professional accountants called Keirishi wereborn in 1927 and this qualification continued until 1967. The number of Keirishi who passed the qualification examination was very few (about 100 in 19 times of examination) and the majority of them were the people who got this qualification without examination (graduates of universities majoring in economics and accounting); the total number of them was 25, 570.The Keirishi Act was enacted in 1927 and was abolished in 1947 when the Certified Public Accountants Act was enacted.
4. CPA qualification was given to people who passed the CPA Examination started in 1951. The Certified Public Accountant Act was enacted in 1947.
5. TA qualification was given to people who passed the TA Examination, CPA and Lawyer qualification holders and retired from NTA. The Certified Public Tax Accountant Act was amended in 1951.
6. We can estimate population, economic activities and other numbers in old times by the research of cliometrics. Cliometrics is one of the research fields of economic history.
7. Economic White Paper in 1956 said included these famous words. It encouraged the Japanese people.
8. Ezra Frivel Vogel (1930-), Professor of Harvard University, made research on Japanese society and got some lessons for US society.

REFERENCES

1. Arrow, Kenneth Joseph, Social Choice and Individual Values, John Wiley and Sons, 1951.
2. Bryant, Stratton and Packard, Bryant and Stratton's Common School Book Keeping; embracing Single and Double Entry, New York, 1864.
3. Certified Public Accountant Act, 1947.
4. Certified Public Tax Accountant Act, 1951.
5. Chandler, Alfred DuPont, Strategy and Structure: Chapters in the History of Industrial Enterprise, MIT Press, 1962.
6. Committee to Survey Core Curriculum, Report of the Committee of Core Curriculum, Association of Accounting Schools, 2010.
7. Diebolt, Claude and Michael Haupert ed., Handbook of Cliometrics, Springer, 2016.

https://link.springer.com/content/

pdf/10.1007% 2F978- 3- 642- 40406-1.pdf

8. Financial Instruments and Exchange Act, 2006. (JSOX)

   http://www.japaneselawtranslation.go.jp/law/detail/?id=1911&vm=&re=02

9. Financial Service Agency, Enforcement Release on Audit Firm and CPAs, 2006.

   https://www.fsa.go.jp/singi/singi_kinyu/kounin/siryou/20060529/ 01.pdf

10. Fogel, Robert William used cliometrics in his research and wrote many books and articles.

    The Union Pacific Railroad: A Case in Premature Enterprise, (Johns Hopkins University Press, 1960).

    Railroads and American Economic Growth: Essays in Econometric History, (Johns Hopkins University Press, 1964).

    Without Consent or Contract: the Rise and Fall of American Slavery, (W.W. Norton, 1989).

    The Fourth Great Awakening & the Future of Egalitarianism, (University of Chicago Press, 2000).

    The Slavery Debates, 1952- 1990: A Retrospective, (Louisiana State University Press, 2003).

    The Escape from Hunger and Premature Death, 1700- 2100: Europe, America, and the Third World, (Cambridge University Press, 2004).

11. Fujinuma Tsuguoki, President's Announcement on Kanebo Accounting Fraud, Association Japanese Certified Public Accountants, 2005.

12. Fukuzawa, Yukichi, translated by Dilworth, David A., An Encouragement of Learning, Keio University Press, 2012.

13. Independent Committee, Olympus Inc., Report on the Independent Committee, 2011. https://www.olympus.co.jp/jp/info/ 2011b/if 111206corpj.html

14. Independent Committee, Toshiba, Report on the Independent Committee, 2015. https://www.toshiba.co.jp/about/ir/jp/news/ 20150721_ 1.pdf

15. International Accounting Education Standards Board (IAESB), IESs, IFAC, 2010.

16. International Accounting Education Standards Board (IAESB), 2019 Handbook of International Education Standards, IFAC, 2019.

    https://www.iaesb.org/publications/2019-handbook-international-education-standards

17. International Ethics Standards Board for Accountants (IESBA), Final Pronouncement – The Restructured Code, IFAC, 2018. https://www.ethicsboard.org/publications/final-pronouncement-restructured-code- 19

18. Investigative Committee on Olympus Audit, Shinnihon Audit Firm, Report on the Investigative Committee, 2012.

    https://www.shinnihon.or.jp/about-us/news-releases/ 2012/pdf/ 2012- 03- 29.pdf

19. Iwata, Iwao, Audit of Professional Accountants, Moriyama Book Store, 1954.
20. Iwata, Iwao, Accounting Principles and Auditing Standards, Cyuokeizai Co., 1955.
21. Keirishi Act, 1927.
22. Kitasato, Shibasaburo, The Bacillus of Bubonic Plague, Lancet, 1894.
23. Kito, Hiroshi, Japanese History discovered from Population, Kodansha, 2000. (Japanese)
24. Public Company Accounting Reform and Investor Protection Act, 2002. (SOX)
https://www.govinfo.gov/content/pkg/PLAW- 107publ 204/pdf/PLAW- 107publ 204.pdf
25. Securities Act of 1933.
https://legcounsel.house.gov/Comps/Securities% 20Act% 20Of% 201933.pdf
26. Securities Exchange Act of 1934.
https://legcounsel.house.gov/Comps/Securities% 20Exchange% 20Act% 20Of% 20 1934.pdf
27. Shoup Mission, Report on Japanese Taxation by the Shoup Mission, 1949.
http://www.rsl.waikei.jp/shoup/shoup 00.html
28. Shoup Mission, Second Report on Japanese Taxation by the Shoup Mission, 1950.
http://www.rsl.waikei.jp/shoup/shoup 51.html
(contents only)
29. Takashima, Masanori, Japanese History of Economic Growth, Nagoya University Press, 2017. (Japanese)
30. Tax Agent Act, 1942.
31. The Economic Planning Agency, Economic White Paper in 1956, The Japanese government. https://www 5.cao.go.jp/keizai 3/keizaiwp/wp-je 56/wp-je 56- 0000i 1.html
32. Toshiba Tec Corporation, Pos System Top
https://www.toshibatec.com/products_overseas/pos_system/
33. Toyoshima, Yoshikazu, History of Cost Accounting at Mitsubishi Shipbuilding Nagasaki, Dobunkan, 2006. (in Japanese)
34. Vogel, Ezra Frivel, Japan as Number One: Lessons for America, Harvard University Press, 1979.

中華民國電腦稽核協會

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

協會簡介

願 景

願景：持續為資訊科技治理與電腦稽核之先導機構。

宗 旨

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

任 務

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

沿 革

- 1994 年 7 月 14 日正式創立，由朱寶奎擔任第一屆理事長。秘書長由林秀玉會計師擔任。
- 1996 年 7 月由朱寶奎續任第二屆理事長。秘書長由林秀玉續任。
- 1998 年 7 月由魏忠華接任第三屆理事長。秘書長由陳瑞祥擔任。
- 2000 年 8 月由魏忠華續任第四屆理事長。秘書長由黃淙澤擔任。
- 2002 年 9 月由蔡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。秘書長由黃淙澤擔任。
- 2014 年 8 月由林宜隆續任第十一屆理事長。副理事長由楊期荔續任。秘書長由黃淙澤續任。
- 2016 年 8 月由張紹斌接任第十二屆理事長。副理事長由蘇庭興擔任。秘書長由黃淙澤續任。
- 2018 年 9 月由張紹斌續任第十三屆理事長。副理事長由蒲樹盛擔任。秘書長由黃淙澤續任。
- 2020 年 9 月由葉奇鑫接任第十四屆理事長。副理事長由蒲樹盛續任。秘書長由黃淙澤續任。

會員權益

一、可免費參加本協會定期舉辦之例會活動 (含台北、新竹、南區)，並獲得 CISA、CISM、CRISC 及 CGEIT 持續進修 (CPE) 學分。

二、參加 CISA、CISM 國際證照考試複習課程及本協會舉辦之課程可享有會員折扣價。

三、會員得以優惠價格購買協會出版品。

四、可免費獲得協會出版之《電腦稽核期刊》(一年兩期)。

五、透過電子郵件方式，可取得電腦稽核相關領域之最新訊息。

六、輔導會員取得國際電腦稽核師 (CISA)、國際資訊安全經理人 (CISM) 、國際資訊風險控制師認證 (CRISC) 及國際企業資訊治理師 (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。

2021 年度下半年教育訓練課程列表

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

課程類別	課程主題	時數	預定開課時間	課程費用
ISACA 國際證照系列	CISA 國際電腦稽核師認證研習班_平日班	30	**9/8-10, 15-16**	NT$ 40,000
	CISM 國際資訊安全經理人認證研習班_假日班	24	**10/16, 23, 30, 11/6**	NT$ 32,000
ISO 系列(與 BSI 合辦)	ISO 27001:2013 資訊安全管理系統 CQI & IRCA 主導稽核員訓練課程	40	**10/4-8、11/15-19、12/6-10**	NT$ 53,000
	ISO 27001:2013 資訊安全管理系統 建置實務課程	24	**10/19-21**	NT$ 36,000
	ISO 20000-1:2018 服務管理系統 CQI & IRCA 主導稽核員訓練課程	40	**12/6-10**	NT$ 55,000
	ISO 20000-1:2018 服務管理系統 CQI & IRCA 稽核員/主導稽核員轉版訓練課程	16	**11/4-5**	NT$ 22,000
	ISO 22301:2019 營運持續管理系統 CQI & IRCA 主導稽核員訓練課程	40	**11/8-12**	NT$ 55,000
	ISO 22301:2019 營運持續管理系統 基礎課程	16	**12/13-14**	NT$ 21,000
	ISO/IEC 29100:2011+A1:2018(CNS 29100)隱私框架 主導稽核員訓練課程	36	**12/20-24**	NT$ 55,000
	BS 10012:2009 個人資訊管理系統 國際標準基礎課程	8	**11/26**	NT$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準建置課程	16	**12/13-14**	NT$ 15,000
內稽系列	編碼有原則－管理無缺口上機設計操作	7	**9/29**＊、**10/27**＊、**11/24**＊、**12/15**＊	NT$ 6,500
	十秒內飆速編製損益表與合併報表	7	**10/20**＊、**12/2**＊	NT$ 3,850
	範例設計五大組成要素之自行評估問卷**(初任課程)**	7	**10/26**＊	NT$ 3,850
	應用商業簡報視覺化技巧呈現經營分析與稽核報告	7	**11/23**＊	NT$ 3,850
	以電腦控制關鍵點查核舞弊實務案例	7	**11/25**＊	NT$ 3,850
	一例一休加班特休目前法規真實範本	7	**12/24**＊	NT$ 3,850
	內部稽核「協助組織達標」有效作法★	6	**9/6**＊	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	**10/1**＊	NT$ 3,300
IT Audit 與資訊治理系列	核決權限制定原則與執行稽核風險管控機制**(初任課程)**	7	**9/28**＊	NT$ 3,850
	用 Power BI 做大數據稽核－採購循環(南部班)	6	**9/6**	NT$ 3,300
	電腦稽核規劃實務**(初任課程)**★	6	**9/7**	NT$ 3,300
	網站安全與稽核簡介(Ⅰ)★	6	**9/16**＊	NT$ 3,300
	網站安全與稽核簡介(Ⅱ)★	6	**9/24**＊	NT$ 3,300
	數位時代電腦稽核實務**(初任課程)**★	6	**10/5**	NT$ 3,300
	資訊系統與通信傳輸查核★	6	**10/6**	NT$ 3,300
	ERP 系統控管與查核實務★	6	**10/8**＊	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 操作)	6	**10/14**＊	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	應用系統導入 PKI 安全機制與檢查	6	**10/21**＊	NT$ 3,300
	談資安事件應變機制及稽核重點★	6	**10/22**＊	NT$ 3,300
	資訊部門稽核與資訊系統控制查核★	6	**11/11**	NT$ 3,300
	數位身分(Digital Identity)風險與挑戰★	6	**11/17**＊	NT$ 3,300
	資料存取於稽核與行為分析之應用	6	**11/18**＊	NT$ 3,300
	網路與系統安全實務查核★	6	**11/19**＊	NT$ 3,300
	ZERO TRUST－管理及內控的跨界治理★	6	**11/29**＊	NT$ 3,300
	雲端世代之科技風險發展趨勢★	6	**12/3**＊	NT$ 3,300
	數位時代下的稽核變革及實務案例分享★	6	**12/6**	NT$ 3,300
	數位時代的採購流程控管與查核實務★	6	**12/9**＊	NT$ 3,300
	行動應用 APP 安全檢測與實務★	6	**12/23**＊	NT$ 3,300
	ISMS 資訊安全管理系統內部控制與稽核	6	**12/28**＊	NT$ 3,300
舞弊稽核與數位鑑識系列	💻利用數位鑑識分析人員不當行為	6	**9/17**	NT$ 3,300
	資安事件與資料外洩鑑識調查實務分享★	6	**10/15**＊	NT$ 3,300
	資安持續稽核與監控：組態安全管理之應用★	6	**10/28**	NT$ 3,300
	認識數位鑑識技術基礎與實務	6	**11/5**	NT$ 3,300
	結合系統資料與網路資源透析潛在舞弊事件	6	**11/12**＊	NT$ 3,300
	不實財報的各種作假手法與鑑識資料分析(FDA)細察技術★	6	**11/30**＊	NT$ 3,300
	數位證據與實例分享★	6	**12/17**＊	NT$ 3,300
個資外洩與保護系列	💻個資法導入與查核內控循環作業管理規範**(初任課程)**	7	**12/16**＊	NT$ 3,850
	資料庫稽核與個資保護★	6	**10/7**＊	NT$ 3,300
	個人資料保護稽核★	6	**12/10**＊	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。
※ 日期後有標註「＊」為「實體」及「線上」同步招生，因是安排在同一天，如有確定開課，屆時會視報名人數及疫情狀況，擇一開班，不會實體+線上混搭。
※ 「初任課程」僅限證期局(公開發行公司)之內稽人員可申報，銀行局、保險局不適用。
※ 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
  ※註：無認列線上課程時數
- ■ 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。
※ 詳細課程規劃請上本會網站 www.caa.org.tw 查詢，或來電(02)2528-8875 洽詢。

電腦稽核期刊前期篇名整理

第四十三期_智慧治理在持續性稽核之創新技術與應用

- 論人工智慧與隱私權保障之研究 - 現代科技與資訊隱私權之拉鋸戰
- 探討網路寫手之偵測方法與研究
- 視覺化與機器學習協同整合之增強分析 - 以風險視覺化為例
- Evolution of Smart Governance-The Past, Present and Future of Governance and Auditing
- 資訊及相關技術的管理、控制與稽核 (COBIT) 於政府部門
- 資訊安全其治理稽核之落實

第四十二期_電腦稽核在新興科技應用的機會與挑戰

- Study of CIM and IoT-Simulation for Cost Performance Analysis-Cost management
- Shodan 為基礎的 IoT 安全等級與防護機制
- 隱私資訊管理系統標準 ISO 27701 於 GDPR 適用性評估
- 人工智慧對於審計實務之影響
- 論全球衛星定位系統於偵查中使用之合法性及立法制度發想
- 物聯網需要更好的安全性
- 區塊鏈存證應用於司法數位證據之芻議

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

近期活動報導

2021.01.26

新竹例會

【 疫情下之風險管理與稽核 】

◆疫情下之風險管理與稽核專題演講 - 安永企業管理諮詢服務股份有限公司魯君禮協理

本次例會邀請安永企業管理諮詢服務股份有限公司魯君禮協理以「疫情下之風險管理與稽核 」為主題，來談疫情對企業營運的影響，以及企業因應的風險管理策略可由三構面 : 網路安全、技術韌性、營運持續性與韌性三階段策略來強化組織應對 COVID- 19 的能力，並討論防疫期間日常作業的防禦手段，如 WFH 該注意的事、如何減緩 BYOD 之風險、如何對惡意攻擊，從各個面向來教大家要如何強化組織應對疫情的能力。

台北例會

2021.01.29

【 物聯網應用與資訊安全 】

物聯網 (IoT) 是被各行各業如金融、醫療等最為廣泛應用的熱門新興科技之一，隨著日漸廣泛，蘊藏的風險已逐漸為人所關注，因為 IoT 的服務更貼近個人，所以也就牽涉到了個人資料保護的議題。本次例會邀請到東吳大學法學院法律學系余啟民副教授，從物聯網的發展與應用、國際相關資訊安全基本標準以及近期發展與未來的挑戰，暢談如何在使用 IoT 科技這個全球性的課題時也能同時兼顧資通安全與個資保護。

◆東吳大學法學院法律學系 - 余啟民副教授

新竹例會

2021.03.25

【 AI- 發現威脅 】

資訊科技進步對生活帶來許多便捷，但同時也帶來資安風險，不論是個人或是組織都可能成為攻擊的目標，個資外洩或企業遭駭客入侵造成損失時有所聞，在資安世界裡，人工智慧（ AI）這場防禦和攻擊的 AI 攻防戰已經開打。本次例會由欣盟科技有限公司產品協銷部 - 張博喬課長來分享資安威脅的演進，資安營運的挑戰，提出全方位 AI 威脅獵捕、自動化流程回應，以及事件分析及改善建議，來說明如何應對已知或預防未知的威脅。

◆欣盟科技有限公司產品協銷部 - 張博喬課長

2021.03.29

【 長照機構運用雲端資訊服務規範與作業指引說明研討會 】

因應衛生福利部近來持續推動長照 2.0 計畫相關工作，並積極擴大服務資源與照顧對象，同時在雲端運算的數位浪潮下，許多長照服務提供者選擇導入雲端服務藉以提升企業的競爭力。在此智慧醫療的蓬勃發展趨勢之下，長照機構如何選擇合適且無虞的雲端產品，以及簽訂具保障之合約書，同時兼顧資訊安全與資料隱私，已為當今亟需探究之課題。有鑑於中華民國電腦稽核協會以及勤業眾信聯合會計師事務所長期深耕台灣照護醫療之資安議題，衛生福利部委託中華民國電腦稽核協會以及勤業眾信聯合會計師事務所，針對長照機構運用雲端資訊服務之潛在資安風險進行研究，並於本次研討會上發表長照業者與雲端服務廠商之間的合約範本與監理框架研究結果。

2021.03.31

台北例會

【 新興科技風險管理與資安控管 】

科技在許多產業被廣泛使用，推動了整個人類社會的發展，進而讓我們的生活更加便利，然而這樣的便利性也伴隨著資安風險增加。本次例會邀請到安侯企業管理股份管理有限公司資訊科技諮詢服務 - 郭宇帆協理，討論在新興科技應用下的法令遵循與風險管理要如何變革、風險評估：框架 ABCD、運用科技進行法令遵循工作：從組織到技術、我們所面對的資安風險與應對模式來瞭解其風險管理與資安控管的重要性與趨勢。

◆安侯企業管理股份管理有限公司資訊科技諮詢服務 - 郭宇帆協理

台北例會

2021.04.26

【 運用國際標準遵循個人資料保護法規稽核實務 】

◆英國標準協會台灣分公司 - 孫文良客戶經理

本次例會邀請英國標準協會台灣分公司 - 孫文良客戶經理，來談「運用國際標準遵循個人資料保護法規稽核實務 」，從隱私保護法制與國際標準之間的關係，介紹隱私資訊相關之國際標準，並舉例說明隱私資訊之國際標準如何應用於稽核實務。資訊發展快速的時代，個人資料保護相關法規成為全球關注之議題，而對企業而言，導入管理系統的價值在於協助組織對齊營運目標，讓隱私保護逐步完善。

2021.05.4~6

【臺灣資安大會（CYBERSEC）】

由 iThome 主辦的「臺灣資安大會（CYBERSEC）」是臺灣最具指標性的資安會議，為亞洲地區舉足輕重的資安交流平台。大會今年以「TRUST: redefined 信任重構」為主題，為期三天的活動，規劃超過 200 場次全方位議題演講，邀請國內外重量級的資安專家齊聚一堂，以前瞻的思維、豐富的經驗、多元化的觀點與嶄新的視野，帶來最完整、最多元資安情報與解決方案，引領大家看見不一樣的資安。

◆中華民國電腦稽核協會 - 葉奇鑫理事長

中華民國電腦稽核協會葉奇鑫理事長，同時也是達文西個資暨高科技法律事務所所長，於會中分享資安風險量化評估工具 ISACA COBIT 2019，讓企業能夠針對組織的業務目標及其具體需求靈活地設計切實可行的治理解決方案，即使企業面臨多種資安風險量化挑戰，如風險評估方法不一致、經驗不足造成資料分析限制，採用 COBIT 2019 的企業將受益於資源利用最佳化、效率提高和更有效的資訊與科技。

2021.05.07

【2021 年全國大專院校電腦稽核個案競賽暨專題研討會 】

◆本屆競賽主辦單位與評審團：左起中華民國電腦稽核協會黃淙澤秘書長、資誠聯合會計師事務所姚慶儒會計師、勤業聯合會計師事務所侯玉燁副總經理、安侯聯合會計師事務所陳怡如副總經理、台北商業大學會計資訊系江淑玲主任、安永聯合會計師事務所黃誌緯協理、審計部温大民組長、兆益數位股份有限公司莊盛祺總經理

全國大專院校電腦稽核個案競賽暨專題研討會為國立台北商業大學所主辦的活動，由審計部、臺灣證券交易所、中華民國會計師公會全國聯合會、中華民國內部稽核協會、中華民國電腦稽核協會、台灣舞弊防治與鑑識協會、安永聯合會計師事務所、安侯建業聯合會計師事務所、資誠聯合會計師事務所、勤業眾信聯合會計師事務所、兆益數位股份有限公司共同協辦。電腦稽核個案競賽由全國各大專院校組隊參加，研討會則以「下個世代內部稽核 - 治理、方法及運用科技技術 」The Next Generation of Internal Audit-Governance,Methodology and Enabling Technology 為研討會主題，活動宗旨在於期望透過競賽啟發會計人對自身專業運用的能力及思維外，也讓實務界及學術界有共同的溝通平台，以利建構國內企業發展電腦稽核技術及持續性稽核與監控的藍圖，並向大家分享全球化與資訊科技發展趨勢。

ISACA

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

取得更多資訊

查閱ISACA認證：www.isaca.org/credentialing

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

證明您在IT/IS稽核、控制和安全方面的專業知識
–提升職能潛力，成為行業中最合格的

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。

目前全球已超過151,000人取得CISA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。

說明
專為資訊科技/資訊系統稽核師，以及控制、保證與資訊安全專業人士設計。

資格要求
至少5年專業資訊系統稽核、控制或安全工作經驗。

考試範圍領域(%)
1.資訊系統稽核流程 (21%)
2.資訊科技治理與管理 (17%)
3.資訊系統的取得、開發與建置 (12%)
4.資訊系統的營運及企業靈活性 (23%)
5.資訊資產的保護 (27%)

將您的職業生涯從技術領域轉移到管理領域
–從戰略角度為企業做出貢獻

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2012年獨立研究Foote Partners的資訊技能與證照報酬指數(IT Skills and Certification 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。

目前全球已有超過46,000人取得CISM認證。

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。

說明
專為管理、設計、監督和評估企業資訊安全的人員設計。

資格要求
至少 5 年專業資訊安全管理工作經驗。

考試範圍領域(%)
1.資訊安全治理 (24%)
2.資訊風險管理 (30%)
3.資訊安全計劃開發與管理 (27%)
4.資訊安全事故管理 (19%)

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。

目前全球已有超過8,000人取得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。

說明
CGEIT對各種專業人員的資訊科技治理原則和實務知識及其應用進行認證。

資格要求
至少 5 年從事顧問或監督職務、或以其他方式支援企業資訊科技相關治理工作經驗。

考試範圍領域(%)
1.企業資訊科技治理 (40%)
2.資訊科技資源 (15%)
3.效益實現 (26%)
4.風險最佳化 (19%)

證明您在企業風險管理和控制的專業能力
–提升職業生涯和薪酬

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。

目前全球已有超過30,000人取得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。

說明
專為具有資訊科技風險管理經驗，並具有資訊系統控制、設計、實施、監督和維護經驗的人員設計。

資格要求
至少3年且其中需有IT風險識別或IT風險評估工作經驗。

考試範圍領域(%)
1.治理 (26%)
2.資訊科技風險評估 (20%)
3.風險回應與報告 (32%)
4.資訊科技與安全 (22%)
※自2021/8/1更新

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「台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「台灣人文及社會科學引文索引資料庫」登錄為第三級期刊。本會為維持期刊品質，推動電腦稽核領域之實務應用與研究，持續於 2019 年參與「臺灣人文及社會科學期刊評比暨核心期刊收錄評比」，此次評比仍獲評為第三級期刊，且分數較上期進步。

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，以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之發展。

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向，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。

**** 投稿說明 ****

- 投稿文章請以中文或英文撰寫，文稿請用 MS WORD 處理。
- 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」)。
- 專業論壇及新知園地除首頁外，皆請依順序編入頁碼，作者姓名及相關資訊僅能出現於首頁。

ISACA
Taiwan Chapter

中華民國電腦稽核協會
11070台北市信義區基隆路一段143號7樓之4
7F.-4, No.143, Sec. 1, Keelung Rd., Xinyi Dist., Taipei City 11070, Taiwan (R.O.C.)
886-2-2528-8875 Fax : 886-2-2528-8876
Web : www.caa.org.tw www.isaca.org.tw