IT查核人員所需的進階資料(或數據)分析

Advanced Data Analytics for IT Auditors

作者： Spiros Alexiou, Ph.D., CISA

Is an IT auditor who has been with a large company for eight years. He has more than 20 years of experience in IT systems and data analytics and has written numerous sophisticated computer programs. He can be reached at *spiralexiou@gmail.com.*

譯者: 周濟群,中華民國電腦稽核協會編譯出版委員會委員

資料分析對於查核功能[1]來說是一種必備能力，且可預期在未來它將成為查核的主要部份[2]。

資料分析的定義如下：「一種檢視原始資料乃致能得出關於資料的結論之科學…」[3]該定義並可延伸如下：

資料科學通常可區分為探索性資料分析與確認性資料分析，前者指由資料中發現新屬性，後者則是由資料證明假說的真實性…在資訊科技領域，資料科學一詞對IT查核來說有特別的意義，尤其是在檢查組織資訊系統、營運和流程相關控制時，資料分析專指系統是否能有效地保護資料、能有效率地運作、並能達成組織整體目標。[4]

不同領域分別會使用簡單到進階的資料分析方法，例如：

- 類別分析－確認好壞顧客或是否舞弊
- 分群分析－確認具備類似行為的群集
- 關聯分析－決定如：買了A商品的顧客同時也買了B商品，而且80%的這些顧客也同時買了C商品
- 彙總分析－描述某些族群具有某些特性（例如：有那些主管級人員使用公司信用卡的平均花費超過x元）
- 鏈結分析－決定連結關係（例如：A打電話給B，接著B立刻打給C，如此可能可將A鏈結至C）
- 偏差度偵測－確認某些交易顯著地偏離平均值
- 預測／估計分析－預測某一新營業項目的未來趨勢或成長率
- 視覺化分析－雖然正確來說，這可能並非資料分析方法，但它可協助非自動化的人類認知發現（例如：圖表或醫療影像）

資料分析的兩大類型

資料分析技術通常可分為下列兩種類型：

- 簡單類型－分析者清楚他要找的是什麼。這種類型的分析通常具有某些明確定義的規則或門檻，以供分析者找尋違反規則的情形（例如：查詢所有金額大於某門檻值的交易或查詢所有退休後仍可再繼續存取IT系統的人員）。此類型分析通常利用資料庫或試算表來執行查詢，一般查核任務廣泛使用本類型分析。當資料量變大時，查核人員通常得依賴IT人員協助彙整資料，這些資

料可能會因為較無彈性且必須依賴IT，而被視為不適切。而此類資料也不需要量大才合用。

- 進階類型－分析者對於他要找什麼並沒有預先設定的知識（例如：查核人員並不會測試是否違反門檻條件，甚至不確定違反規則的門檻為何）。例如，查核人員會發現尚未被任何已知規則或門檻涵蓋的新情況，查核人員更有興趣發現趨勢或模式，或是新知識。這類資料通常在說一個故事，因此查核人員必須能讀懂這個故事。典型的例子如舞弊－對一些新形式的舞弊，查核人員可能無法明確知道查核是否存在且究竟什麼構成了該舞弊。查核人員可能更有興趣去教電腦如何讀懂這些資料並做出推論，當然這類電腦程式必須受到監督。

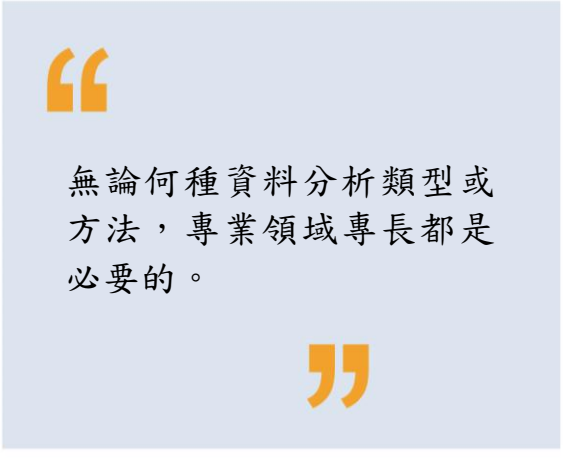
第一類型資料分析類似於利用規則來學開車（例如：如何啟動引擎、如何煞車、如何轉動駕駛盤、了解速限），而第二類型則類似於觀看影片來學習什麼是好的或什麼是不好的駕駛技術。在第二類型分析中運用的資料分析方法通常是結合了第一類型和第二類型，而本文即著重於此類型的進階資料分析。

進階資料分析的複雜度

進階資料分析主要處理無法被某些簡單規則如：「若某交易金額大於一個給定的值且分析者過去未曾發現這類交易歷史，則將其歸類為可疑的。」來標示的複雜案例，這些簡單規則通常會設定門檻值且將超過門檻視為一種指標。但老練的舞弊通常會規避被第一種類型資料分析技術所建立的簡單規則所偵測到，而進階資料分析技術則專門針對此類有趣的案例。例如：雖然短期間通話本身可能並不可疑，但若與其它資訊合併則可能成為電訊或專用交換機濫用的警訊。通常來說，雖然一項未被偵測的入侵威脅或舞弊行為可能因為不會違反單一規則或門檻而可以避開第一類型分析，但該活動必定仍會呈現某些可被進階資料分析偵測到的異常特徵。進階資料分析甚至可以在正常行為尚未定義為規則或門檻時，協助偵測到偏離於正常行為的事件。然而，為了達成此目標，所有攸關資訊（如：資料欄位）皆必須被確認且包含於資料集合中，即使某資訊可能還無法清楚地關聯到某一舞弊行為。

需要領域專長的案例

無論何種資料分析類型或方法，專業領域專長都是必要的，這也是企業在聘任新查核人員時之所以要求他們必須具備如IT或財務專長的主因。



在確認攸關資料欄位時，領域專長是必須的。若提供不攸關的資料給系統與資料分析工具，則傳回結果必為噪音，而且調查誤報的成本通常很高。例如，某企業利用資料分析確認舞弊行為、洗錢或可能攻擊時，資訊科學家能夠了解並應用資料分析工具，但卻未必能知道和使用所有攸關的資料欄位。但領域專家則能做出資訊是否攸關或可能攸關於舞弊、洗錢、攻擊、入侵等，但他們卻未必知道在複雜案

例中，應使用何種資料分析方法。

一定要成為資訊科學家才能使用資料分析工具嗎？

簡單的回答是不用。理想上，分析者要能知道如何指示系統或工具去「針對資料集合 B 執行方法 A，並提供結果。」很多工具都能協助查核人員完成。「企業的前十大資料分析工具」[5] 提供了一個資料分析工具清單，本文會介紹當中大部份的工具，這些工具的主要差異則在於使用容易度、介面和價格。

資料分析工具的使用者必須能夠：

- 了解方法A能做什麼
- 準備好資料集合B以供方法A使用
- 詮釋結果

為了能使用這些分析工具，必須先對資料分析的某些專業術語有所認識，因為這些方法或其子方法多數使用技術名稱，如：序列最小優化算法、支援向量機和K平均演算法（最廣泛使用的分群演算法）。

資料準備

通常來說，一個資料集合若包含以下特性，則必須執行資料準備：

- 超過一個欄位（如：貨幣值和交易筆數）
- 非數值類別欄位（如：男性／女性）
- 名義欄位，如：公司內職位（管理者、董事、資料輸入人員）

資料準備提供各欄位對程式或工具的相對重要性，如：由一般使用者所建立的10筆交易相對於由管理者所建立的10筆交易之重要性。另一個例子是與銀行間交易筆數相對於所有交易金額總數，兩者間同等重要嗎？還是總交易金額較重要？若是如此，重要性高出多少？需要領域專長的資料準備工作類似於定義一個共同尺度來衡量不同的數量，當資料集合包含非數值資料，如答案像是“這筆匯款是否有可疑的收款地？”此類是／否欄位時，這項工作可能會更加複雜，因為必須將此一非數值資料轉換成能夠呈現其相對重要性的數值。

由於很多方法使用距離（亦即衡量兩個事件所具備特性或交易欄位值的相近程度）的概念，所以將相對重要性數值化是必須的過程。每個事件包含數個欄位，各欄位值需為數字且尺度足以代表相對於其他欄位的重要性。這也就是為何此項工作需要領域專長，沒有任何程式聰明到可以自行決定相對重要性，除非有人告訴它。

資料分析方法

雖然可用的方法很多，以下五種資料分析方法被認為可提升查核品質：

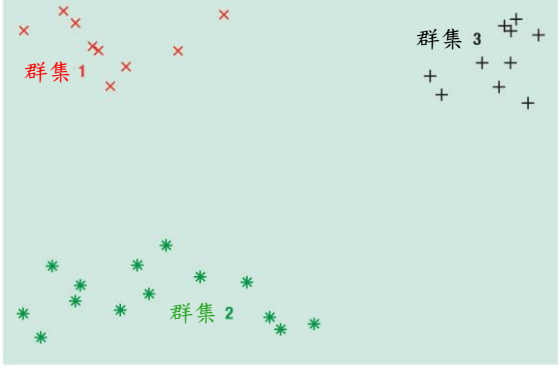
分群

分群將資料組織成幾個類似的群集，例如：

- 某一群經理的工作委外行為類似且不同於其它經理
- 某一群客戶的消費行為皆屬於交易次數多但交易金額小
- 具有特殊屬性的IP封包

分群自然地將具有相似屬性的資料集合成一群，並與其它群中的資料區分開來。圖1展示具有兩個屬性的資料分群結果，資料被劃分至圖中三群中的某一群集（X, *, +）。

圖 1–具有兩個屬性的資料分群



Source: Spiros Alexiou. Reprinted with permission.

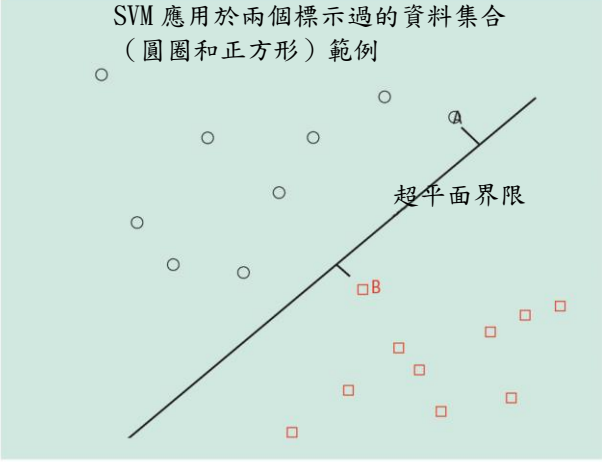
若目標是欲了解每個群集的意義，則必須由人類進行後續分析與詮釋，諸如群集重心、每群集平均值和資料屬性值的散佈程度。分群需要一項良好定義的距離來衡量相似的行為。雖然能夠指出某些事件距離其它同群事件較遠（極端值），但分群並無法確認奇怪或可疑的群集，因此必須由人類來詮釋和了解分群結果。分群是一種幾乎不需要任何假設的探索性工具，它可以廣泛地應用於會計查核至網路流量查核。[6, 7, 8] 例如，分析曾被應用於將網路流量區分為正常和異常的兩群集[9]。每個群集內的元素的封包、位元數和其它不同的來源—目的地配對等特徵值，皆較接近於同群內其它元素，而離其它群集內元素較遠。

支援向量機

支援向量機(SVM)資料分析方法和分群類似，因為SVM會盡可能準確地定義不同群集間的界限，例如：舞弊／非舞弊或有償債力／無償債力。SVM與分群的主要差異在於SVM使用標示過的資料集合來訓練電腦繪出界限，在數學上來說，這界限叫做超平面。SVM定義的超平面／界限可以最佳方式將兩個標示過的資料集合分開，且可極大化兩邊資料集合靠界限最近的兩點距界限間的距離合，如圖2所示。如此，落在界限左邊的新事件就可被分類為左平面的類型（如：舞弊／非舞弊、對新資訊系統的正面／負面意見）。

圖2展示SVM應用於兩個標示過的資料集合（圓圈和正方形）。作為界限的超平面將兩個資料集合以最佳化方式分開，亦即它極大化了兩邊資料集合靠界限最近的點A與點B距界限間的距離合，SVM是一種具有堅實數學基礎的穩定方法，且可使用相對少量資料集合來訓練。然而對使用者來說，其分析結果並非完全透明可見，而且此方法對於離界限最近的標示點（如圖2中的點A與點B）非常敏感，一個在學習／訓練資料中錯誤的標示可能導致錯誤的分析結果。因此，SVM最適用於目的是要找到界限，且分析者對於已知案例（特別是界限附近的點）的標示有足夠信心的情況，例如：償債能力分析、入侵偵測和財報驗證。[10, 11, 12]

圖 2– SVM 應用於兩個標示過的資料集合（圓圈和正方形）



Source: Spiros Alexiou. Reprinted with permission.

案例式推論

案例式推論（CBR）方法嘗試由高階層次模仿人腦的推論過程，常見的問題解決方法像是檢視醫生、技師和律師如何處

理一個問題，CBR即會在資料庫中儲存問題的解決方法，以便在遇到新案例時，使用相同的推論過程來尋找類似問題的解決方法（圖3）。

新案例建立的規則是根據其與資料庫中已知案合的鄰近程度，因此CBR的一個缺點是當新案例距離所有目前已知案例皆甚遠時，它可能會被誤認。實務上，該決策或分類不會只根據一個最鄰近的已知案例，而是使用一些最鄰近案例（k-NN），如此可緩和因已知案例不足所帶來的可能錯誤影響。CBR方法使用良好定義的距離來衡量兩個案例的鄰近程度。使用CBR有一個重要的好處是它的透明度－主要因為其分析結果是根據與已知案例X的鄰近程度，因此，CBR對於分類一個與過去經驗相近的新案例最為有用，且最能加以解釋。

在實務上CBR的例子從辨認可疑交易到會計與銀行查核皆有[13, 14, 15, 16, 17]，例如，藉由分析系統呼叫發生頻率，研究者可以辨認入侵行為[18]，而藉由登入記錄分析，則可辨認內部使用者異常的系統濫用。[19]

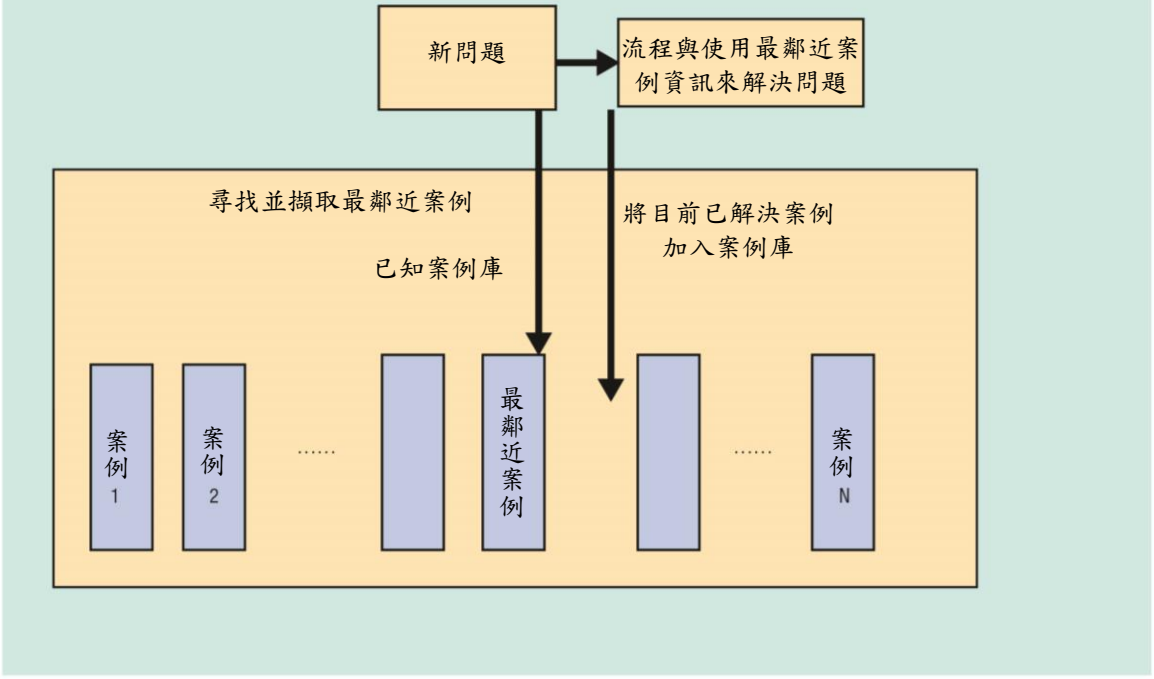
類神經網路

類神經網路（ANN）資料分析方法嘗試由低階神經元層次來模仿人腦，只要給定學習或訓練用資料集合（輸入），AAA可以生成一個能產出已知結果的網路（輸出）。當新的資料集合輸入時，可預期ANN網路可以正確地預測輸出。因此，ANN可被視為一種複雜、多維的內插方案，該方法利用現有的輸入輸出對應，來預測在同一值域中，對應至其它輸入的輸出值。此方法的最大缺點是它對人類來說是不透明的，無法提供為何預測該輸出一個簡單的解釋。此缺點對許多應用來說是很關鍵的，包括查核，因為如果報導了一項發現（如：舞弊），其相關細節卻令人無法了解，這是不可接受的。然而，ANN還是被廣泛地應用，包括查核[20]。如何應用ANN於查核工作在文獻中有很多例子，包括使用公開可得的舞弊財報資料來偵測管理舞弊[21, 22]，對某件值得調查的事來說，使用ANN作為指標可能是很有價值的。

隨機森林

隨機森林資料分析方法是決策樹方法之一，決策樹嘗試由現存已評估（已標示）的案例來發展規則。例如，某演繹出的規則可能像是當獨立審計委員會存在且每年至少開會兩次時，財報錯誤會降低。然而，決策樹常會因為使用了所有資料屬性而發生過適現象。例如，決策樹可能使用了完全與最終結果無關的資料來形成規則。隨機森林則是一種使用了很多樹的改良方法，每一個決策樹僅使用一部份資料屬性，它的設計可緩和決策樹的過適問題以及對噪音過於敏感的問題，它使用平均數來避免噪音。這個方法和管理上的德爾菲方法[23]有點類似，德爾菲透過意見的遞迴改善將數個專家的意見收斂至單一答案。或許一個更好的類比是普選或公投，我們可以假設多數選民是理性的，但他們個別可能對某些議題並不理性，同理，在森林中的多數決策樹在處理大部份資料時可被視為好的，但對少數資料可能產生不同的隨機錯誤，若期待的結果是一個數字，則我們將所有樹的平均值當做森林的平均值，若答案應為是或否，則多數決議即為結論。如此，隨機森林可以基於已標示案例，提供人類能了解的規則，來對現有或未來案例進行分類。

圖 3 案例式推理的應用



Source: Spiros Alexiou. Reprinted with permission.

隨機森林工具通常是非商業化的，它們可使用相對少量而多屬性的資料產出不錯的結果。一個最近的例子是應用隨機森林於財務舞弊偵測，他們利用許多指標如：債務比率、流動比率和毛利率等來建立規則。[24]

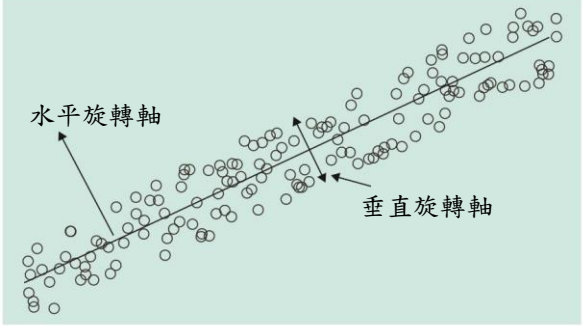
降低複雜度的主軸或主成份分析法

將分析結果以最簡單詞彙讓人了解永遠都是重要的，因為結果必須解釋給管理者知道。通常來說，資料紀錄包含許多欄位來描述一個事件（如交易或登入目的）的各種屬性，主軸分析是一種能減少攸關欄位數的數學方法。例如，資料分析方法可能偵測某種舞弊或其它有趣行為具有高交易量、小金額的特徵，至於其它屬性則多數不相關，本例中包含了一個由舞弊圍繞著的主軸，另一軸則可能描述另一種舞弊且包含其它屬性組合，則該軸為另一主軸。

圖4是主成份分析的一個釋例：該資料呈現多數的變異是沿著水平旋轉軸而非垂直旋轉軸，其結果是，忽略垂直旋轉軸所相對失去的資訊很少，因此我們可以降低本問題的複雜度至單一變數（水平旋轉軸）而不需要兩個變數。

主軸分析可以協助人類了解，因為大多數變數是沿著軸的，因此較易了解並視覺化。一個簡單的例子是入侵，進入時點和離開時點原本個別並非攸關變數，但兩者間差異則很重要，因此若能指出較長時間的入侵，則不同的軸集合可帶來更多資訊。

圖 4 主成份分析



Source: Spiros Alexiou. Reprinted with permission.

從兩個不同世界找到最佳解

通常來自不同類型的分析方法會結合起來使用，以規則為基礎的第一類型方法（分析者知道他要找什麼）通常較快速、簡易，且多為結論性的。第二種類型方法（分析者並不一定準確地知道他要找什麼）通常需要密集計算、在資料準備和詮釋上更為複雜，且多為指示性的。因此，查核人員通常會先使用以規則為基礎的方法，然後再針對不易分類的案例使用第二種類型方法。

目前有非常多的分析工具可供使用，且許多是免費的，這些工具可能成為查核工具箱的重要增添品。

曾有人說：「ANN和CBR系統已證明它們以更低的成本，為大型會計師事務所提供了較佳的查核效率、查核品質，並可降低查核風險。現在正是查核人員使用這些工具的時機。」[25]雖然每個查核個案不同且各自具有各自的需求，但許多查核可能可由使用簡單和進階資料分析獲益。

應用這兩種類型分析可以用低成本來改善異常偵測，因為多數工具是免費的開放來源碼。例如，研究者可結合他們的CBR分類器與簽名驗證來分析系統呼叫發生的頻率以確認入侵[26]。傳統工具可有效用於白清單中的案例，因而加快分析過程。此外，由進階分析結果可與規則或門檻基礎的分析結果整合，例如，具有某些屬性的網路流量配合上異常的流量群集，可能被標示為可疑的。

許多資料分析技術與工具可以顯著協助查核人員發現資料中隱匿的知識、驗證假說並最大化資料價值。這些資源最好能和查核人員（或其它可能團體）的領域知識，以及傳統工具相結合。這些工具中許多是免費的，而且對查核人員來說易於使用，只要查核人員明確知道他們要如何處理這些資料。

“
這些資源最好能和查核人員（或其它可能團體）的領域知識，以及傳統工具相結合。
”

END NOTES

1 EYGM Limited, “Harnessing the Power of Data:How Internal Audit Can Embed Data Analytics and Drive More Value,” EYG no. AU2688, October 2014, *www.ey.com/Publication/vwLUAssets/EY-internal-audit-harnessing-thepower-of-analytics/$FILE/EY-internal-auditharnessing-the-power-of-analytics.pdf*

2 Izza, M.; “Data Analytics and the Future of the Audit Profession,” ICAEW, 22 April 2016,*www.ion.icaew.com/MoorgatePlace/post/Dataanalytics-and-the-future-of-the-audit-profession*

3 Rouse, M.; “Data Analytics (DA),” *TechTarget*, January 2008, *http://searchdatamanagement.techtarget.com/definition/data-analytics*

4 *Ibid.*

5 Jones, A.; “Top 10 Data Analysis Tools for Business,” KDnuggets, June 2014, *www.kdnuggets.com/2014/06/top-10-dataanalysis-tools-business.html*

6 Thiprungsri, S.; M. A. Vasarhelyi; “Cluster Analysis for Anomaly Detection in Accounting Data: An Audit Approach,” *The International Journal of Digital Accounting Research*, vol. 11, 2011, p. 69-

84, *www.uhu.es/ijdar/10.4192/1577-8517-v11_4.pdf*

7 Munz, G.; S. Li; G. Carle; "Traffic Anomaly Detection Using K-Means Clustering," 17 January 2016, *https://www.researchgate.net/publication/242158247_Trafc_Anomaly_Detection_Using_K-Means_Clustering*

8 Dhiman, R.; S. Vashisht; K. Sharma; "A Cluster Analysis and Decision Tree Hybrid Approach in Data Mining to Describing Tax Audit," *International Journal of Computers & Technology*, vol. 4, no. 1C, 2013, p. 114-119

9 *Op cit*, Munz

10 Auria, L.; R. A. Moro; "Support Vector Machines (SVM) as a Technique for Solvency Analysis," DIW Berlin, German Institute for Economic Research, August 2008, *www.diw-berlin.de/documents/publikationen/73/88369/dp811.pdf*

11 Abd Manaf, A.; A. Zeki; M. Zamani; S. Chuprat; E. El-Qawasmeh; *Informatics Engineering and Information Science, International Conference*, ICIEIS 2011, Proceedings, Springer, 2011

12 Doumpos, M.; C. Gaganis; F. Pasiouras; "Intelligent Systems in Accounting," *Finance and Management*, vol. 13, 2005, p. 197-215

13 Curet, O.; M. Jackson; "Issues for Auditors Designing Case-based Reasoning ystems," *The International Journal of Digital Accounting Research*, vol. 1, iss. 2, p. 111-123, *www.uhu.es/ijdar/10.4192/1577-8517-v1_6.pdf*

14 Liao, Y.; V. R. Vemuri; "Use of k-Nearest Neighbor Classifier for Intrusion etection," *Computers and Security*, vol. 21, 2002, p. 439-448

15 Denna, E. L.; J. V. Hansen; R. D. Meservy; L. E. Wood; "Case-based Reasoning and Risk Assessment in Audit Judgment," *Intelligent Systems in Accounting, Finance and Management*, vol. 1, iss. 3, September 1992, p. 163-171

16 Ho Lee, G.; "Rule-based and Case-based Reasoning Approach for Internal Audit of Bank," *Knowledge-Based Systems*, vol. 21, iss. 2, March 2008, p. 140-147, *http://dl.acm.org/citation.cfm?id=1344916*

17 Singh, A.; S. Patel; "Applying Modified K-Nearest Neighbor to Detect Insider Threat in Collaborative Information Systems," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, iss. 6, June 2014, p. 14146-14151

18 *Op cit*, Liao

19 *Op cit*, Singh

20 Chao, H.; P. Foote; "Artificial Neural Networks and Case-based Reasoning Systems for Auditing," *Accounting Today*, 2 July 2012, *www.accountingtoday.com/news/artificialneural-networks-case-based-reasoningauditing-63178-1.html*

21 Koskivaara, E.; *Artificial Neural Networks in Auditing: State of the Art*, Turku Centre for Computer Science, February 2003, *http://citeseerx.ist.psu.edu/viewdoc/wnload?doi=10.1.1.67.459&rep=rep1&type=pdf*

22 Fanning, K. M.; K. O. Cogger; "Neural Network Detection of Management Fraud Using Published Financial Data," *Intelligent Systems in Accounting, Finance and Management*, vol. 7, 1998, p. 21-41

23 Rand Corporation, Delphi Method, Rand.org, *www.rand.org/topics/delphi-method.html*

24 Liu, C.; Y. Chan; A. Kazmi; S. Hasnain; H. Fu; "Financial Fraud Detection Model Based on Random Forest," *International Journal of Economics and Finance*, vol. 7, iss. 7, 25 June 2015, p. 178-188, *https://mpra.ub.uni-muenchen.de/65404/*

25 *Op cit*, Chao

26 *Op cit*, Liao

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 6, 2016 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2016,Volume 6中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Copyright

© 2016 of Information Systems Audit and Control Association ("ISACA"). All rights reserved. No part of this article may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ISACA.

版權聲明：

© 2016 of Information Systems Audit and Control Association ("ISACA"). 版權所有，非經ISACA書面授權，不得以任何形式使用、影印、重製、修改、散布、展示、儲存於檢索系統、或以任何方式(電子、機械、影印、或錄影等方式)發送。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每

年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得 ISACA 的書面許可。如有需要，欲複印 ISACA Journal 者需向 Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取 2.50 元美金固定費用，每頁收取 0.25 美金。欲複印文章者則需支付 CCC 上述費用，並說明 ISACA Journal 之 ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經 ISACA 或版權所有者許可之複製行為則嚴明禁止。