行政院國家科學委員會專題研究計畫　成果報告

設計同步稽核資訊系統雛型以支援 B2B 電子商務環境下之內部控制(I)

計畫類別：個別型計畫
計畫編號：NSC91-2416-H-263-001-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：致理技術學院會計資訊系(科)

計畫主持人：林鳳儀
共同主持人：梁德容
計畫參與人員：紀東昀 郭明泉 黃俊閎

報告類型：精簡報告

處理方式：本計畫涉及專利或其他智慧財產權，2 年後可公開查詢

中　華　民　國 92 年 10 月 17 日

行政院國家科學委員會補助專題研究計畫■ 成 果 報告　□期中進度
報　告

設計同步稽核資訊系統雛型以支援 B2B 電子商務環境下之內部控制

Design an Continuous Auditing Information Systems to Support the Internal Control Under B2B Electronic Commerce

計畫類別：■ 個別型計畫　□ 整合型計畫
計畫編號：NSC　91－2416－H　263 －001　－　－
執行期間：　91 年　08　月 01 日至　92　年　07　月 31 日

計畫主持人：林鳳儀
共同主持人：梁德容
計畫參與人員： 紀東昀 郭明泉 黃俊閎

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年■二年後可公開查詢

執行單位：致理技術學院會計資訊系

中　華　民　國　　92　年　07　　月　31　日

摘　　要

觀察全球產業發展趨勢，電子商務將蓬勃發展，而隨著科技資訊的進步，投資人對會計師師及時揭露財務的需求，以及防範舞弊等功能的要求也愈來愈高。審計人員在查核財務報表時，如何運用新興科技以持續地覆核與監控受查企業，乃成為一項重要之議題。

傳統的會計資訊系統因為受制於各受查者之資訊系統的開發時間不一、使用不同程式語言設計、或架設在不同平台上，以至於喪失各應用系統間的互動性（Interoperability）與資訊傳遞，使得同步稽核技術的發展十分困難。然而隨著 Internet 及 B2B 電子商務環境下之較具透明化與結構性之管理流程與相關技術發展，由會計師事務所開發其與受查客戶間的同步稽核資訊系統，以提昇稽核的品質，已不再是昂貴而遙不可及的事。因此，如何利用現有資訊技術，建構一個應用於企業間（B2B）電子商務之稽核資訊系統模式，並採用同步稽核之概念，以有效地審查電子商務交易內企業會計資訊系統之互享，已成為電腦技術的一項重要挑戰。此外，資訊安全的威脅除了技術層面外，資訊系統內部控制政策也是相當重要的一環，因而激發本研究之動機。

首擬先建構一套可運用於 B2B 電子商務之稽核系統雛型，本系統乃採用 ebXML 為交換資料的標準，HTTP 與 SOAP 基礎，實作一個同步電腦稽核系統雛型，以有效稽核 B2B 之電子商務。再深入地探討此稽核環境下之安全需求、

風險及資訊系統之內部控制目標，並參考 COBIT 架構，設計 B2B 電子環境下對受查客戶之電腦稽核要求，並以實際製造業電子商務個案為例，說明如何將所設計之內部控制制度與同步核資訊系統架構相結合，達成以同步稽核資訊系統支持電子商務環境下之內部控制目的。

關鍵詞：電子商務、會計資訊系統、電腦輔助稽核技術、SOAP、COBIT

English Abstracts

As the increasing dependency on electronic commerce (EC) transaction, auditors are required to disclose the financial statement at continuous basis in order to prevent Internet fraud effectively. Therefore, how the auditors take advantage of modern technologies in order to provide continuous audit and review process has become an important issue. The integration of many existing EDP system to assist computer audit is a daunting task due to the following facts: 1. Traditional accounting information systems (AIS) were developed with different computer languages at different time. 2. The AIS has been deployed on different computing systems and/or platforms at different time.

It is important for CPA firms to adopt the most advanced Internet technologies in order to enhance B2B EC audit quality. We therefore partially facilitate the continuous auditing information system by message distribution middleware such as simple object access protocol (SOAP), which is one of the four information technology infrastructures that facilitate EC. Enterprises also requires a comprehensive set of internal control for its IS to pinpoint the security concerns.

We propose a continuous auditing information system prototype based on which new Internet technologies can be incorporated to audit modern B2B EC system. This prototype adopts XML (including ebXML, XBRL), HTTP, and SOAP so that the interoperability issues of disparity EDP system can be addressed. Then, we propose the internal control issue for information system (IS) and utilize the COBIT framework to set the IS checkpoint under the B2B EC environment. This may facilitate the concurrent auditing concepts that are long believed difficult in implementation.

Keywords：E-Commerce, Accounting Information system (AIS), Computer-Assisted Auditing Techniques (CAATs), SOAP, COBIT

壹、計畫背景

電子商務（Electronic Commerce）近年來以驚人的聲勢顛覆了人們從事商業行為（Business Conducts）的方式。根據 Forrester Research Inc.等公司的研究報告，企業間電子商務（B2B EC）佔全體企業商業交易之比率將從 1997 之 0.2%，快速成長至 2003 之 9.5%，其產值更高達 1 兆 3 千億美金（$1.33.Billion）。而台灣近年來主要是以高科技製造業出口為導向，根據同樣的調查報告顯示，高科技交易依賴電子商務之比率遠高於一般傳統產業，至 2003 預計 39.3%之產值將來自於電子商務〔26〕。

Dalton, Hill and Ramsey（1994）研究指出，近年來各大會計師事務所的平均訴訟成本高達其審計總公費的 12.5‰ 投資人對於會計師揭露財務資訊的需求以及稽核企業舞弊等功能的要求愈來愈高。而隨著電子商務產值的增加，電子商務環境下的審計風險也就亦形重要。Glover & Romney（1998）認為電子商務環境下的重要工作乃是持續性地覆核與監控，以達成同步稽核之目的。Vasarhelyi 等於是在 1999 提出連續性審計研究報告（CICA and AICPA 1999），其內容包含：（一）認定連續性審計的特質，（二）界定連續性審計範圍，（三）提示與連續性審計相關的各種問題，包括風險評估、意見簽發、新興科技以及其它規範的檢討等，（四）探討連續性審計的各種可行方案等，足見會計權威單位對同步稽核技術之重視〔13〕。

然而，理想的同步稽核系統，必須是動態而又有彈性的系統，會計師事務所的資訊系統必須能與受查企業的系統相整合，而不會增加太多的建置與維護成本，對方在原有的資訊系統上也不應有太大的改變，而能進一步進行資料的截取與監督〔28〕。此種同步稽核技術的困難度比整合企業內部不同的應用系統還要複雜，因為會計師事務所與不同企業間之作業系統、程式語言、通訊標準、資料結構，都可能有很大的差異。過去有許多企業透過加值網路如 EDI 等來從事企業間的資料交換，然而其成本較高，且不是即時性的資料交換，效益難免受阻。現在由於網際網路的快達發展，通訊協定（Protocol）TCP/IP 已成為各個網路彼此交換訊息的標準，因此只要遵循 TCP/IP 協定來構建網路，便能讓訊息（Message）透過網際網路無遠弗屆地順利傳遞。加上 XML 已成為資料標準格式，以及許多標準化的中介軟體，利用分散式物件技術可將不同的應用程式做適當的整合。因此本研究首先以 XML（ebXML 及 XBRL）及 Simple Object Access Protocol（SOAP）技術嘗試建構 B2B 電子商務環境下之同步稽核模式，藉助 SOAP 能透過 HTTP 傳遞的特性，達成跨平台使用電腦輔助稽核系統的目的〔40〕。如此會計師在執行審計工作時，便可不必受限於受查企業使用不同的應用軟體、平

台之限制，而能直接透過 Internet 上的適當授權及時取得客戶資訊。另外利用 XML 制訂出會
計師界的文件標準，從而簡化重複輸入資料之限制，並可設計適當的輔助稽核程式〔49〕。此一稽核資訊系統的形成，會計師與受查企業對彼此流程及交易等訊息擁有通透性，會計師可藉由此稽核架構透過 Internet 對受查客戶之各式資料、應用程式與文件執行審計工作並對交易內容執行持續性地監控與複核，從而提昇審計之品質。

電子商務稽核模式的另一個重要議題就是資訊系統的安全控管問題〔Gantz 1999; Wood 1998; Kalakota & Whinston 1997; Bhimani 1996〕。網路交易時代趨勢，資訊安全威脅如影隨形，依照歐美國家發展經驗分析其原因可歸納二個來源：

1. 來自內部威脅：包括承包商及內部員工，員工又分人為疏忽及犯錯、心懷怨恨及不誠實有意舞弊，而內部威脅佔 80%。
2. 來自外界的威脅：包括 Internet 漫遊者、產業間諜、競爭對手及外國政府、地下組織等，拜電子商務之賜，財務欺騙及資訊財產的竊取越來越容易，此種威脅約佔 20%。

由此可知，電腦資訊安全絕不是單純的技術問題，許多存在於現實狀況中之安全漏洞，其實是源自內部管理層面需求不明確所造成，因此在考慮組織內的資訊安全架構時，內部稽核尤其是電腦稽核亦是一個重要的議題。此外，電子商務之運行是由眾多廠商提供之軟、硬體設備共同運作，使得資訊不僅在組織內傳遞，且在不同組織間的傳遞也愈來愈頻繁。Ryan & Brodoloi 便指出主／從架構和傳統大型系統，所面臨的潛在安全威脅是不同的。受查客戶資訊系統的整體安全若僅依賴安全的網路科技，如：安全的網路協定（SET、SSL）、認證（Authentication Service）、加密技術（Password and Access Control）、防火牆軟體（Fire wall）與實體設備控制等仍顯不足。必須配合良好的內控稽核系統才能發揮其應有的效益；尤其 B2B 電子商務乃建構於開放式的網路之上，受查客戶的主機資料極易暴露於公眾網路上，因此資訊系統的安全與風險控制更是會計師從事電腦稽核的重要。

為降低網路上查核之風險，除了安全科技的輔助外，會計師應設計一套資訊系統環境下之內部控制政策，來偵測環境的漏洞及風險，以減少公司的損失。因此本研究的第二個目的便是適當地規劃電子商務環境下查核受查企業之資訊系統內部控制政策，期能做到及早偵知異常交易狀況，使網路上查核的風險降至最小。傳統交易模式中，會計師事務所為企業進行內部控制評估時，所主張之內部控制作業，主要參考 COSO 委員會（Committee of Sponsoring Organization of the Treadway Commission）之「內部控制 - 整體架構」（Internal

Control-Integrated Framework)。但在電子化企業資訊管理及資訊技術（Information Technology; IT)的內部控制評估作業上, COSO 報告中缺乏實際運作之理論架構及步驟；因此，國際電腦稽核協會（Information System Audit Control Association; ISACA ）提出資訊技術管理之內部控制理論（Control Objectives for Information and Related Technology；COBIT)。

本研究分成二個部分進行，第一部分首先以 Simple Object Access Protocol（SOAP）及 XML（含 ebXML 及 XBRL）技術以建構 B2B 電子商務下之同步稽核模式；第二部分則設計此稽核環境下之內部控制政策、風險、控制目標與架構，並擬以本研究建置之同步稽核資訊系統支援受查客戶資訊系統（Information System; IS）內部控制。

一、研究動機

第一部分：建構同步稽核資訊系統架構架構---XML（ebXML 及 XBRL）；SOAP

Vasarhelyi & Halper （1991）〔45〕認為線上交易的網路資訊系統，可以透過同步稽核系統達成下列目的：

（1） 滿足時效性：在同步稽核的系統下，可即時預防與偵測異常事項的發生，並及時加以因應。
（2） 提高稽核效率，稽核人員可透過事先定義的稽核規則來縮小稽核範圍，並將重點放在異常的事件稽核，而不是龐大、複雜資料的收集。

AT&T 貝爾實驗室在 1991 年曾提出一個連續性流程稽核系統（Continuous Process Audit System; CPAS），來從事電腦審計的工作。然而本稽核系統的缺點為：(1）該系統主要的應用平台是 UNIX 系統，而非網際網路分散式環境。(2）系統開發的方式並非採用物件導向分析或元件架構方法，因而較不具彈性。(3）CPAS 功能僅侷限於內部稽核功能，而非一個完備的連續性審計技術架構，因此並未得到審計實務界的重視。

余千智、周濟群〔民 86〕〔4〕將電子商務環境下之審計分成二類，即期間性審計模式與連續性審計模式。前者乃是應用若干電子交易安全防護技術，如數

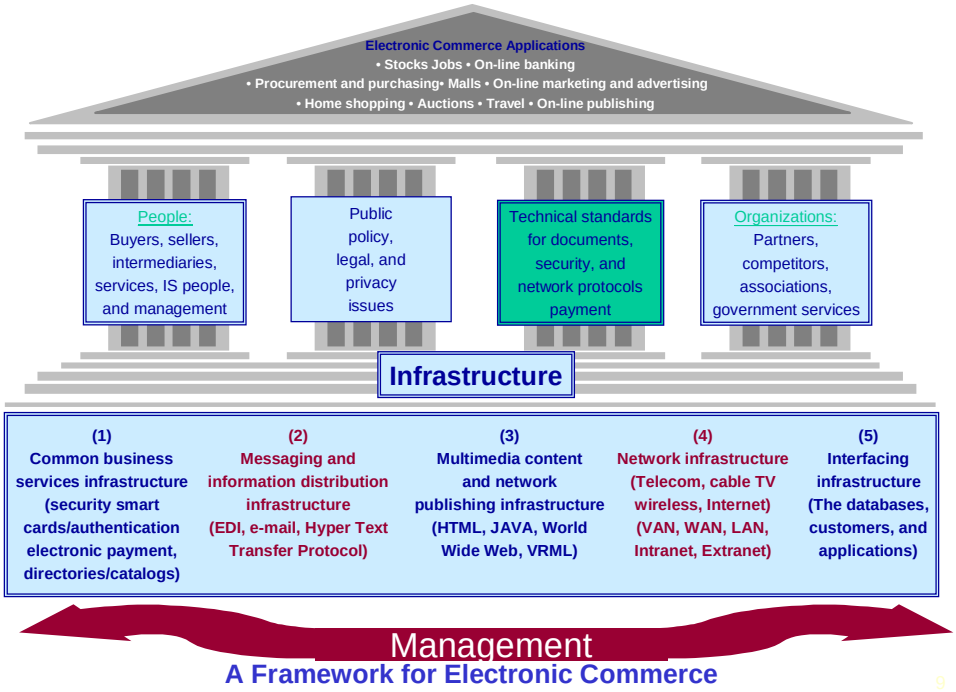
位簽章、資料加密方法等，提供審計人員安全的資料擷取的管道以及權威性的確認技術。至於連續性審計模式，則透過建立於客戶會計系統作業流程與審計人員之間的交易即時監控系統，可供審計人員隨時偵知及報告異常的交易情況，藉以維護會計系統作業及流程的安全，並保障財務資訊即時公開的正確性。

由上述文獻的背景討論可知，儘管過去已有研究試圖探討同步稽核資訊系統，但畢竟此一課題仍屬新興階段，故仍有許多未盡之處。例如同步稽核系統如何在毋須更動受查企業之 EDP 系統下完成？是否可在開放式的環境中應用？以及應運用何種新興科技術最能達成同步稽核之目的？

傳統的會計師事務所多屬大型、專屬的資訊科技架構，加諸一般受企業之應用系統因開發的時間不一，使用不同的程式語言設計，以致各應用系統間的互動性（interoperability）不足，很難建構一個適用於企業間的電子商務稽核系統模式。然而會計師若能利用受查企業在 B2B 電子商務環境下，透明且完整的生產流程管理，同時搭配後端的電子供應鏈機制，則可順利地在開放式的環境中，進行網路上的同步稽核，以提昇審計的效率及效果。

本人於民 89 年曾提出一套以 CORBA 為基底輔助會計師稽核資訊系統之架構，借助新興科技的應用，以物件導向、網路安全、智慧代理人與 CORBA 為基底之分散式架構，以輔助審計人員在封閉性系統下，如何存取受查企業資訊並建構一稽核資訊系統。並於 90 年又提出一套以 XML-based 為資料交換標準，並採用 CORBA 規格為基底，藉由 XML 互通性特性，以物件導向之網際網路程式語言 Java 實作與一個電腦輔助稽核系統，以有效稽核企業與企業間之電子商務，此兩項研究之績效亦已陳述於我們所提交之研究報告中。然而上述研究之稽核架構僅能從事後稽核或期間性的查核工作，尚無法達成同步稽核之目的，另外此系統架構要求會計師與受查企業均須採用 CORBA 作為中介軟體，但 CORBA 目前尚無法直接透過 HTTP 傳遞，因此在 B2B 電子商務環境下的可行性較低。

隨著開放式網際網路應用環境的興起，新發展的 XML（eXtensible Markup Language）標準及 SOAP 平台，因具有能讓使用者自行定義、描述文件資料格式與結構、資料再用性（Data useable and portable）及可跨越不同企業平台作業等特性，不但改進了先前 EDI 的缺失，且大大提昇了在 Internet 環境下與會計師間之資料交換作業的效能。B2B 的電子商務通常特別強調企業端的整合運作，通常較具結構化，以既定的合作關係為基礎，重視關係之維繫，有利於會計師業建立同步之稽核系統架構。



圖一　電子商務之基本架構

根據 Zwass 之研究顯示〔49〕，電子商務之建置主要依賴 5 組底層基礎技術（Infrastructure），如圖一所示，他們分別為（1）Common Business Service Infrastructure，（2）Messaging and Information Distribution Infrastructure，（3）Multimedia Content and Network Publishing Infrastructure，（4）Network Infrastructure，and（5）Interface Infrastructure。其中第（2）項極為一般資訊業界所稱之分散式中介軟體（Distributed Middleware），近年來具代表性的中介軟體及技術包含了 OMG 的 CORBA 〔43〕，Microsoft 之 DCOM〔28〕，SOAP

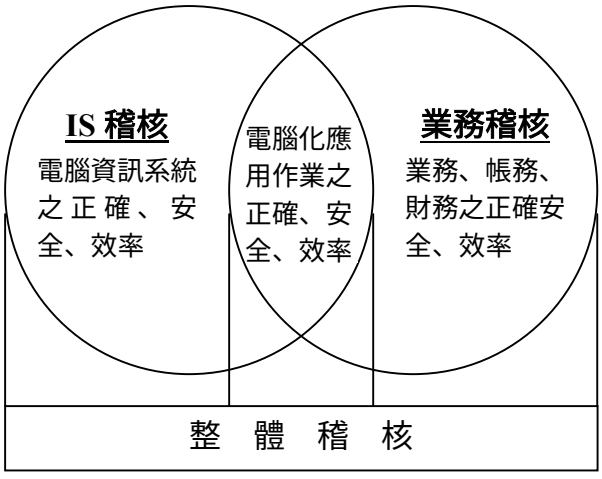
〔40〕以及 IBM 之 MQ 等等。在 B2B 之電子商務中，SOAP 技術最被看好，原因有下列幾點：1.SOAP Base On HTTP，幾乎可被任何類型的防火牆所接受；2.SOAP 具備高度的延展性；3.因為 SOAP 依附於 HTTP，因此，它可應用一些 HTTP 的特色，如 Proxy，SSL 等。因此 SOAP 技術較目前之其它中介軟體更具彈性，未來將成為電子商務世界之主流。

因此本計畫的第一個目的即探討以 SOAP 為基礎，XML（含商務使用的 ebXML 及財務報表使用的 XBRL）為資料交換標準，擬建構一個在 B2B 電子商務交易環境下的同步稽核資訊系統模式。簡而言之，本計畫先從資訊環境較具結構且完整的 B2B 電子商務活動中，探討資訊架構所造成的衝擊和變遷，藉以推導出適用於一般會計稽核業務和符合 B2B 電子商務資訊特性的稽核資訊系統架

構，做為會計師業發展電腦審計工作之參考。此外，由於 SOAP 可依附 HTTP，因此當會計師在取得受查企業資訊時，可直接藉由 HTTP 之介面取得生產流程管理與電子供應鏈之資訊，並再加以轉換成稽核之資訊，受查企業可在既有的系統下與會計師稽核資訊系統相整合，而不需增加太多的建置與維護成本，再藉由特殊程式之設計對企業進行連續性的監督與複核，因而使得實務界採行同步稽核架構的可能性大增。

第二部分：電子商務環境下，探討同步稽核之安全與內部控制問題---IT Security；COBIT

Internet 的廣泛運用加強了遠距市場的範圍與速度，大幅降低市場的交易成本及複雜性，根據資訊工業策進會的調查研究結果顯示，截至 1998 年 5 月，已有 34.3%的企業建置的網際網路，但伴隨而來之內部控制、資料儲存、稽核軌跡之處理方式改變，已帶給稽核人員莫大的衝擊。而且在電腦犯罪日益增加，稽核人員畏懼電腦的隱憂下，如何加強電腦稽安全控管教育，有效防範電腦作業疏失與舞弊，以確保電腦資源之有效運用，防止電腦舞弊的問題發生是會計師亟待努力的方向。若依整體稽核功能分類，稽核業務可分為業務稽核與資訊系統（IS）稽核兩類，業務稽核係執行業務、帳務及財務等項目之查核，必需精熟各業務手冊規定；而 IS 稽核則著重於稽核硬體、作業系統、應用軟體、資料庫、通訊網路等電子資料處理之控制與管理。業務稽核雖與電腦稽核各司其職，而就防範舞弊及財務報表誤述的角度來看，查核人員則需「業務知識」與「電腦知識」兼修，二者各就其專業能力，共同合作、發揮所長，以收相輔相成之效。（請見圖二，整體稽核示意圖）。



圖二　整體稽核示意圖

林鳳儀〔28〕認為網路安全係指防止網路上傳遞的動態資訊被竊聽、偽造更改與重送等，為防止上述攻擊，網路安全技術必須達到下列功能：

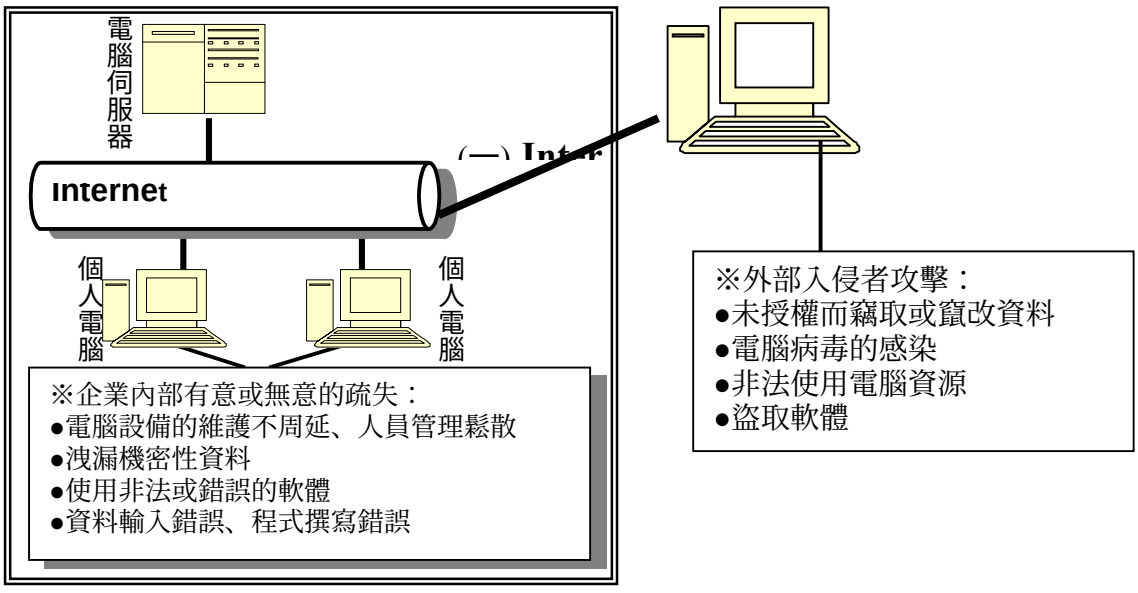
（一）隱私性（Privacy）：防止非法者從網路上得知通信內容。
（二）認證性（Authentication）：接收方可確定資訊來源的合法性；亦即此資訊確實由發送方所傳送，而非偽造或利用過去的訊息來重送。
（三）完整性（Integrity）：接收方可確定接收到的訊息沒有被有意或無意的更改，及被部份取代、加入或刪除等。
（四）不可否認性（Nonrequdiation）：發送方在傳送一訊息後，不可否認其傳送的資訊。

依據電子貨幣安全措施報告（Report of the Task Force on Security of Electronic Money）（Sofia, 1999），認為電子貨幣系統安全的風險及甚控管的方式主要可分為下列三大類〔49〕：

1. 阻檔（Prevention measures）：包括被竄改的防止、文件加密、線上授權、交易確認的加強，主要作業人員的管理與監督。
2. 偵查措施（Detection measures）：如交易軌跡的可驗證性與監督，內部系統的相互牽制，電子貨幣移轉的限制和資金流向的統計分析。
3. 牽制措施（Containment measures）：金額儲存的限制，裝置有效期限的控管，發行者或主管機關被授權對使用者的註冊控制。

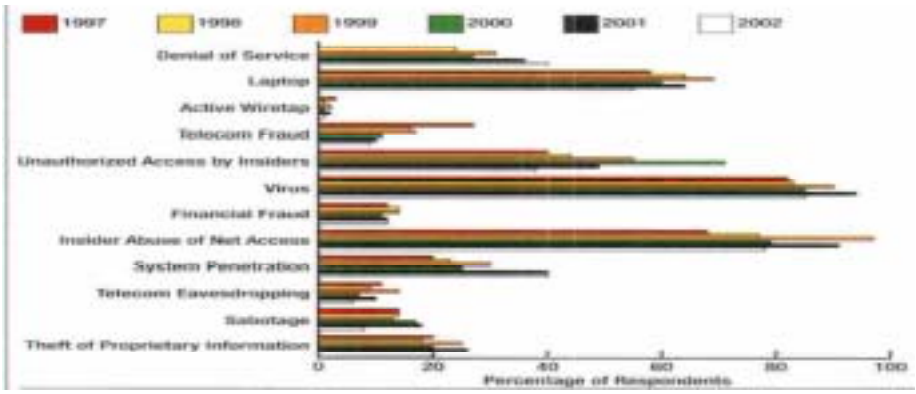
所謂的資訊安全主要是指與電腦相關的資源，例如：電腦軟硬體配備、周邊配備以及網路安全皆包含在內。各學者、專家對於資訊安全的各項定義如下：Dam and Judith Wesley（1997）認為電腦的安全性旨在探討電腦環境軟硬體元件的損害，而目的在於資訊的保密性（confidentiality）、完整性（integrity）、可取得性（availability）、合法性（validity）；吳琮璠、謝清佳（2000）認為電腦的安全管理旨在保護電腦資源，包括硬體、軟體、資料、人員，以防止變更、破壞電腦資源及未授權使用電腦資源；Kees Jansen（2002）認為軟體的應用安全指

的是只有透過認證程序及系統認證的合法人員才可以使用,安全方面指的是隱私權、機密性、責任的分離、身分鑑定、認證及授權。就資訊安全的定義來看，可發現有關資訊的安全與控制可分為兩面:技術面的安全控制與企業內部的安全架構。技術面的安全控制包括防火牆、資訊傳輸與身分認證等機制;企業內部控制面的安全架構則指電腦資源保護與使用者合法性等。而綜合各專家、學者所分類的各項資訊安全的破壞來源，可分成企業內與企業外兩種，如圖三所示：



圖三 資訊安全的破壞來源

根據美國電腦安全協會 （Computer Security Institute; CSI）針對網路攻擊及濫用的調查統計中(圖四)發現 , 來自組織內部的威脅遠大於組織外部的威脅。



可瞭解資訊技術愈發達 , 對於資訊安全的管理愈重要 , 因而資訊安全與管理制度絕對是密切相關的 , 唯有完善的控制制度下 , 才能避免資訊安全的威脅並提昇企業的經營效率。因此 , 企業如何做好資訊安全的控制及管理 , 便成為一項很重要的課題。

圖四 網路攻擊及濫用的統計

由於電子商務組織係建構於一個開放性網路，以提供客戶各種服務的資訊系統，因此，其內部控制目標已不僅限於 COSO 報告之達成營運效率及效能、財務報導之可靠性以及相關法令的遵循三大目標，而應更廣泛的涵蓋品質及安全需求。

因此，國際電腦稽核協會 ISACA（1998）〔23〕提出對資訊系統內部控制的 COBIT 資訊技術（Information Technology，簡稱 IT）控制的架構，以輔助企業

針對現有資訊系統執行內部控制之稽核。COBIT 對於資訊系統內部控制訂定了效能、效率、機密、完整、可用、遵循及可靠等七大目標，且為達成七大目標而劃分了四大範圍，在此範圍中明訂了 34 項控管作業，其主要資訊技術（IT）之資源包含：

（一）資料（Data）：廣義的含括了外部與內部、組織與非組織、圖形、聲音等。

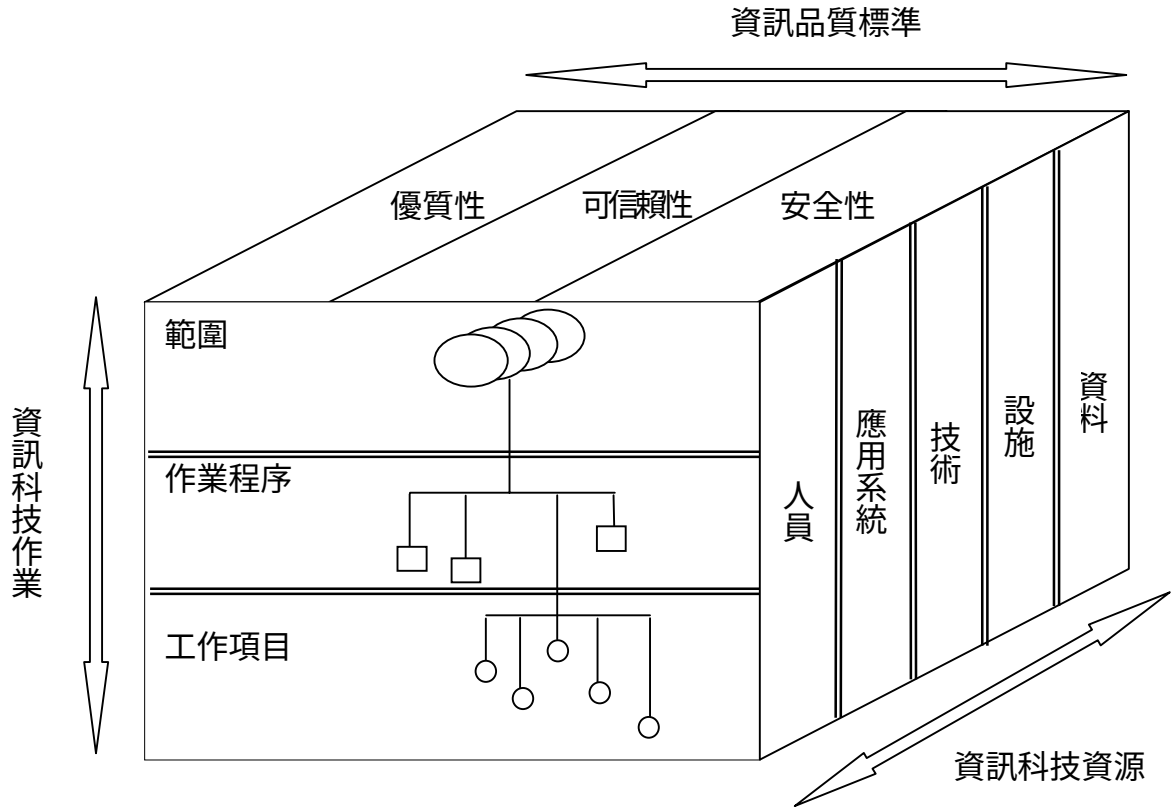
（二）應用系統（Application Systems）：其含意概括了人工和電腦程式規劃程序在內。

（三）技術（Technology）：包括硬體、操作系統、資料庫管理系統、網路、多媒體等。

（四）設備（Facilities）：保存與支授資訊系統之資源。

（五）人員（People）：行政技術、計畫之了解與執行。

COBIT 為確保營運需求與資訊技術上的結合，因此重新對控制策略予以重新定義，並應用執行與監督的手法來管制這些資源，以確保組織可以滿足他們本身對於資訊技術上所提出的個別需求。以下即為營運需求與 IT 控管目標所必需的架構（如圖五）。



圖五 COBIT 營運活動與資訊技術控管目標
資訊來源：ISACA〔1998〕〔23〕

COBIT 的五大資訊技術資源為：

1. 人員：包括對於規劃、組織、取得、傳遞、支援、及監督資訊系統及服務的技巧、認知及生產力。
2. 應用系統：了解手冊的要點和設計的程式。
3. 技術：包括硬體、操作系統、資料庫管理系統、網路、多媒體等。
4. 設備：包括建築物及支援資訊系統的所有資源。
5. 資料：其定義很廣，包括內部的、外部的、圖形、聲音等。

在開放式的網路系統上，受查企業之資料極易直接暴露於公眾網路上，因此安全技術與內部控制將成為未來會計師事務所稽核資訊系統架構的重要考量因素。而 COBIT 係一套系統化、結構化之資訊系統控管及評核標準，較 COSO 更有助於審計人員評估受查企業資訊系統之範圍、權責、方法及技術方面等全方位考量，使審計資源能作最有效之規劃。因此本研究將深入研究受查客戶資訊系統之安全需求、風險及資訊系統內部控制目標之相關理論，並參考 COBIT（Control Objectives for Information and Related Technology；COBIT）的內控架構技術來加強電子商務稽核系統之風險管理與安全控制〔14〕，並擬積極地檢視 COBIT 之資訊安全政策、內部控制以期將之與本計畫第一年建置之同步稽核架構相結合，使會計師得利用本計畫第一年建構之稽核資訊系統，持續地監督與複核受查企業之內部控制。

二、研究重要性

在電子商務日益普及的環境下，會計師面臨同業競爭壓力、利潤率下降及人員成本居高不下等因素，再加諸社會大眾及政府機關對簽證品質的要求日趨嚴格，審計人員所遭受的衝擊，除了審計軌跡消失、內部控制方法改變之外，查核風險亦相對提高。由傳統 IT 角度來支援的電腦輔助稽核技術，已無法因應電子商務的環境，審計人員若無法隨著趨勢而調整其審計模式，並從整個稽核資訊系統的 Infrastructure 來思考，而僅就現有系統疊床架屋，在新興電子商務科技源源不斷地產生、企業起而效尤的同時，會計師的審計業務將無法滿足企業及社會大眾之需求。林鳳儀等〔27〕〔28〕之研究指出目前的稽核資訊系統要作到輔助會計師同步地查核受查客戶資訊，最大的問題在於系統整合的困難，因此，如何利用新興科技與同步稽核技術以增進稽核效率與審計服務品質，勢必成為未來的趨勢。

此外，當開始使用電子商務時，必須發展新的稽核策略來評估組織的功能。在最低限度之下，審核電子商務的應用系統，應斟酌及檢查所選擇使用的電子

商務系統的過程，顧客服務的水平、安全、網頁的維持和監控，網頁提供和風險分析。而安全問題是電子商務稽核的最大障礙，Ryan 與 Bordoloi（1977）指出，傳統大型主機與主從式架構之資訊系統，其安全威脅來源有極大之差異。使用資訊安全不僅應考慮資訊技術層面，更重要的是從制度面來考量，建立適用於組織之 IS 內部控制策略。因而引發本文擬探究網路之安全與風險問題，並採用由電腦稽核協會（Information Systems Audit and Control Association）制定之資訊及相關科技之控管目標，簡稱 COBIT 的內部控制架構本計畫之於網路稽核架構中。茲將本計畫之重要性列示如下：

1. **整合同步稽核審計理論和相關的資訊技術**：以系統性的方法進行彙整，發展出適用於同步稽核的一般化技術架構。本階段整合電腦審計的相關技術包括評估同步稽核之資訊架構、貝爾實驗室之 CPAS、內部控制的 COBIT、以及各種與同步稽核相關的領域知識。
2. **運用 ebXML 與 SOAP 為基礎實作一個運用元件技術之同步稽核架構雛型系統，以增進查核效率並降低審計風險**：本計畫首先配合 Extranet 網路架構，再以 SOAP 透過 HTTP 傳遞的特性達成跨平台及防火牆的阻礙，使受查客戶毋須在會計師之資訊系統採用相同的平台標準，會計師可自 HTTP 上自由取得受查客戶資訊。同時藉由訊息內容為 ebXML 格式的特性建立標準的資訊交換及傳遞模式，使得所有會計帳物件可以透過 ebXML 及 SOAP 跨越各種工作平台及網路通訊協定互相傳遞，克服過去會計師在執行電腦審計時受制於受查客戶異質 EDP 系統之限制。如此一來會計師便可透過網際網路隨時同步地取得受查客戶之資訊，從而增進查核效率，並進一步降低審計風險。
3. **充分利用元件開發方法，強化資訊系統的相容度及彈性**：未來稽核資訊系統架構將受到電子商務及虛擬企業觀念的影響，而物件導向的程式設計方式可以說是新一代系統建置的主流。這樣的趨勢運用在極度強調安全性的會計師業資訊系統，更可以發揮其短小精幹的特性。透過元件化的方式，將稽核的運算邏輯封裝於不同的物件之中，可減少系統大幅修改的需要。此外，充分運用元件化的物件來執行所需要的交易要求，可使系統更具彈性與可管理性。
4. **採用分散式物件設計毋須更動受查客戶之舊有 EDP 系統（legacy system）**：由於分散式物件具有高延展性、擴充性、通透性、自動化與開放性等特性。因此，本計畫所提出之稽核資訊架構不但可有效輔助目前的同步電腦輔助技術，且可利用分散式物件資訊截取（information intercetion）之優點，使審計人員隨時調整其查核策略而毋須更動受查客戶之舊有 EDP 系統。
5. **運用同步稽核技術（Continuous Auditing）及時監控受查客戶之交易，以降低審計風險**：利用內嵌式稽核模組（Embedded Audit Modules）透過 B2B 電

子商務下的快速回應系統（QR）、電子表單、供應鏈管理（SCM）、需求鏈管理（DCM）等資訊及網路運用，來截取高風險區的資料，當某些違規交易發生時，系統自動產生例外報告（Exception Report），亦可針對某些重要交易設計交易追蹤（Transaction Tagging）的模組，以持續檢核交易控制的程序。並且充分和企業內部的既有系統或作業流程緊密結合。本計畫將設計一套具有同步稽核功能，運用 plug-and-play 的方式在適當的電子商務交易控制點上，插入會計師專屬之稽核模組，從而強化稽核作業處理的效率，有效地降低查核風險，並提昇服務品質。

6. **利用日誌（logging）或特殊的控制軟體來覆核系統軟體：**作業系統、排序拷貝等公用程序、程式館軟體、存取控制軟體等，可運用日誌來評估系統的安全及系統資源是否曾被有效運用，亦可利用軟體工具如 CA-Examine、SAS、SPSS、Focus 等來檢核系統軟體，查詢分析系統軟體的參數設定及密碼的使用控制。
7. **提出對稽核系統之安全設計及內部控制方針：**B2B 電子商務環境下之安全與風險迥異於傳統稽核業務，尤其電子商務的資訊稽核架構係建構於開放的傳輸系統，因此安全需求是同步電腦審計能否順利推展的主要考量因素，本計畫擬由過去相關之研究，探討有關電子商務環境下之安全需求與 IS 內部控制方針。
8. **提供會計師在資訊安全技術與 IS 內部控制的整體檢測功能：**藉由蒐集大量技術資訊，參考 COBIT 架構，提供審計人員一個較完整的輪廓，對於會計師而言，科技細節部分並非其稽核重點，可以仰賴專家來評估。但對 IS 之內部控制政策及持續監控的整體概念，可以提供安全的電子商務稽核模式。在會計師業建構本架構下的稽核資訊系統模式之後，由於會計師與客戶之間資訊的互動極為便利，因此將更有餘力去從事其他高附加價值的服務，如顧問諮詢、舞弊查核、內部控制等活動，也更能提供專業化的服務。而 IS 稽亦可保護公司資源，防止內部控制不當的缺失。

三、研究目的

本計畫第一部分之目的為設計一個能夠跨平台、跨區域的協調與整合系統，運用 SOAP 規格透過 HTTP 傳遞的特性造成跨平台使用之目的，而 SOAP 較其它中介軟體系統，更適當於會計師的稽核系統，其理由於其可跨越防火牆的阻礙，使會計師可以自受查客戶的網頁上取得適當的授權，從而開展一個會計師業應用於企業間（B2B）的電子商務稽核資訊系統模式。在此系統下審計人員在取得受查客戶資訊時能夠不受時間、地點限制，也毋須更動客戶之舊有系統（legacy system）而仍能順利地進行高品質的稽核工作。

在前文中，我們已經說明選擇 SOAP 作為我們研究主題的原因，根據我們初步的研究，在現今 SOAP 的標準下，並未針對不同行業稽核與安全應用的相關議題多加著墨，這對於想以 SOAP 為底層通訊機制來建置稽核資訊系統平台將是一大缺失。雖然我們過去曾經以 CORBA 作為資訊系統架構之平台，但 CORBA 與 SOAP 技術上有許多不同點。例如：CORBA 伺服物件的物件參照（object reference）技術在 SOAP 的技術上是沒有的。而 SOAP 因為主要應用於 Web Service 上，因此 SOAP 是以 Web 常用之 Uniform Resource Identifier（URI）來代表網路服務的所在參考位置。換言之，SOAP 在限制上就比 CORBA 少，且 SOAP 可直接透過 HTTP 達成跨平台的效果，因此對於 B2B 的受查企業而言，即毋須再另外建置一套符合 CORBA 標準之平台，而使審計人員可直接透過網路上認證授權後取得受查客戶之資訊。因此本計畫之目的在於利用分散式元件（distributed component）技術，提供一套 SOAP 標準以滿足稽核人員稽核之需求進而達成同步稽核之操作目的。

貳、文獻探討

文獻部分擬先整理現有電腦輔助與同步稽核技術之內容與研究結論，接著針對網際網路之安全性及稽核資訊系統所使用之現代科技，如分散式物件、網路機制上之 XML、SOAP 等作一系列之介紹，另外針對電子商務環境下衍生之資訊安全議題、COBIT 架構等作深入探討，並說明其在電腦稽核上之應用。

一、電腦輔助與同步稽核技術

1. 陳章正

本計畫認為電腦作業可能有下列因素，可能使得控制工作不易執行：(1) 資料處理集中化，此需以程式處理控制取代若干傳統人工制度下的職能分工控制；(2) 傳統稽核軌跡之改變；(3) 資料集中儲存容易失竊、竄改及毀損；(4) 錯誤或舞弊所造成的損失更具嚴重性等。在電腦作業下，一旦程式發生錯誤，可能直至發現時才可能被改正，其錯誤或舞弊已累積多時，所以其造成的損失與影響也較為嚴重；(5) 新的錯誤來源，如：電腦供應商的電腦設備有瑕疵、硬體故障或系統程式錯誤等。

2.Halper, Snively, & Vasarhelyi（1992）

在持續監控軟體的稽核應用方面，AT&T 貝爾實驗室提出一個持續流程稽核系統（Continuous Process Audit System: CPAS）目的是為大型財務系統提供一個整合性的診斷功能，大型電腦系統的稽核與管理通常是分散由不同員來執行，因

此會有一些人需要詳細瞭解
各個系統模組之間是如何運作，但通常是沒有人對系統的整體運作有通盤的瞭解，為了要幫助這些人能快速瞭解並掌控各系統模組之間的協調運作，必需有一個稽核系統將來自於各個不同系統存模組的資訊加以及時有效地整合。CPAS 的系統架構想分為三層：資料供應層次（Data Provisioning Level）、知識層次（Knowledge Level）、與展示層次（Presentation Level）分別說明如下〔45〕：

1．資料供應層

此資料負責資料的擷取，資料的來源主要有三種方式:

(1)由稽核人員或經理人透過第四代語言如 FOCUS，直接存取資料庫。

(2)由監督程式所產生的報表。

(3)由各應用系統所產生營運報告的資料篩選。

2．知識層

(1)系統本身的知識（Knowledge about the System Itself），包括系統功能檢視（Functional View），以及各其間需要透過監督程式各個應用系統加以擷取整合的作業資訊（Operational Information）等。

(2)資訊分析的知識（Knowledge about How to Analyze the System），包括如何編輯（Interpret）每日的資料，如某個時點系統活動快照的檢視格式，以及系統長期問題的辨識等。

3．展示層

將系統所蒐集整理的資訊，透過三種工具來展示：

(1) 流程圖（Flowchart），可以階層式地展示系統功能架構及各個系統模組之間的主要資料流程。

(2) 矩陣（Metrics），存放各系統模組輸入/ 輸出之測量值與標準值，若超出標準值，則顯示警告訊息。

(3) 統計分析圖（Analytics），矩陣之間某些關係的描述，如某日資料的快照（Snapshot）分析，或某段期間的時間序列分析。

3.張俊文（1993）

本計畫針對公開發行以上公司及金融機構之內部審計人員，調查 13 種電腦輔助審計技術的使用狀況。其結果顯示：(1) 內部審計人員使用電腦輔助審計技術並不普遍；(2) 使用電腦輔助審計技術與企業電腦化程度、電腦資訊系統控制的強弱、外部會計師是否使用電腦輔助審計技術、企業擁有電腦稽核專才之人數等因素有顯著差異。

4.劉盈樂（1994）

探討國營事業與民營企業之內部審計人員參與電腦稽核作業的程度及所運用技術，以及對電腦輔助審計技術熟悉程度。研究結果發現（1）較常使用的電腦輔助審計技術的前三名分別為系統發展階段控制指標、自行設計審計程式與公用程式。(2) 技術熟悉度在各行業間並無差異，而與審計人員的學歷有關。(3) 國營事業上市與否確實會影響其對電腦稽核的熟悉度。

5.林鳳儀（2000）

本研究主要在探討新興的資訊科技技術如物件導向、網路安全技術、網際網路技術、及分散式物件規格等，如何輔助會計師從事電腦稽核的工作，以解決過去受查企業之 EDP 系統因缺乏整合性而使審計人員無法順利執行電腦輔助審計技術之困擾，並提出一個立基於分散式物件規格 CORBA 之技術，以及此稽核資訊系統的實施步驟。本研究最後以一金融機構的管理稽核個案為例，說明如何利用此稽核資訊系統架構，實作相關之 CORBA 環境下相關的標準介面與稽核模組。

6. Yu et al.（2000）

本研究探討在電子商務環境中，審計流程所可能受到到衝擊，包括電子商務審計合約的接受、審計風險評估、內控及證實測試執行的方法及時間、審計報告的涵蓋範圍等。他們同時提出諸多新的審計風險及新的內部控制要點，其中新風險乃是經由下列情況而增加：交易個體間的經濟相依性提高、交易與應系統間的相依性提高、交易軌跡消失的可能性增加、交易環境對第三經濟個體的依賴性提高、電子交易資料傳遞的安全與隱密性降低等。而新的內部控制問題則包括：電子交易資料傳遞的安全性、交易處理過程的交易軌跡維護與控制、數位簽章等新技術的控制、網路交易應用系統的應用控制、一般控制與預防控制、評估第三經濟個體內部控制等等。為了解釋電子商務交易系統中各種內部控制程序的運作方式，在他們提出的「Periodical Auditing Process Model, PAPM」中，乃進一步地將余千智與周濟群（1997）的電子發票驗證技術，適當地納入企業的交易處理流程（買方企業的採購循環），以及會計師的事後審計過程中。因此，PAPM 對於電子交易技術在交易流程、審計流程中的應用，提出一個更明確的模式。

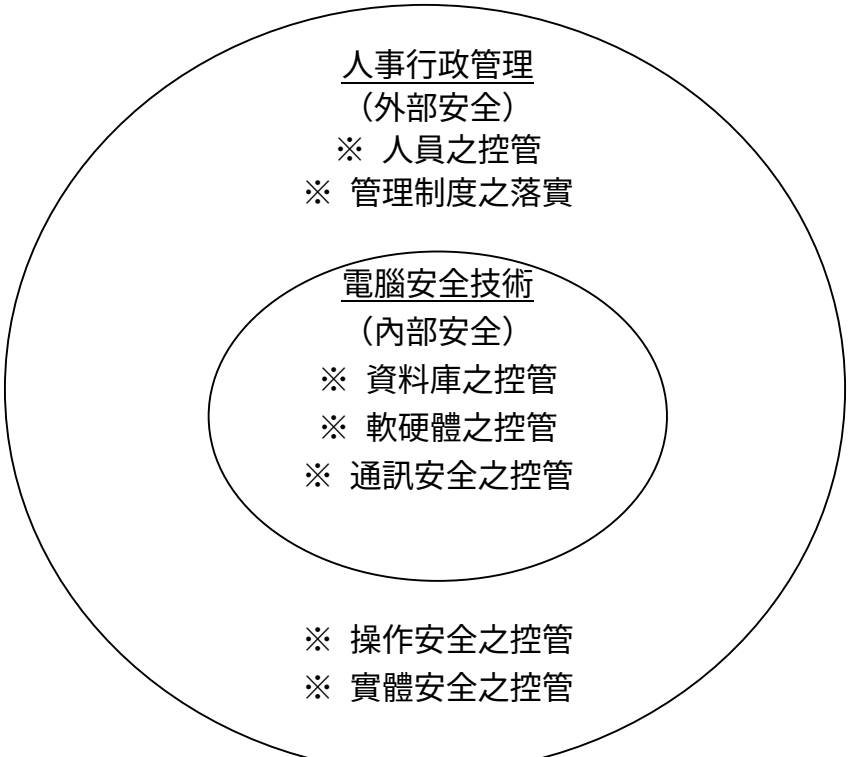
二、資訊安全之管理

資訊安全管理即是為了達到資訊安全之目的所做的控管。陳永裕（1994）整理出有關資訊安全之內容：

1. 電腦安全之控管：在電腦系統的軟硬體設施中加上保護措施。如：加強使用

者身分辨識、資料的存取有嚴格的控制、稽核紀錄、機密資料的加密、檔案備份及定期更新等。

2. 通訊安全之控管：網路系統的軟硬底設備中加上保護措施，以確保資料傳送的安全。如：將資料以加密的方式傳送、身份的驗證系統、伺服器或工作站的人員近出限制等。
3. 實體安全之控管：放置電腦的週遭環境的控管。如：電腦中心應設置在易發生天然災害的地區、完善的保全設備、電腦加裝不斷電系統、門禁的管制等。
4. 操作安全之控管：以確保系統的正常運作。如：系統建置、電腦維修、災難復原、一套標準的作業程序並嚴格執行等。
5. 人事行政之控管：根據許多的紀錄顯示，由於太重視技術性的防護而忽略人員及行政管理的重要性，導致內部人員才是破壞系統安全的主因。其措施應包括：高階主管的親自參與、對系統相關人員的背景深入了解、系統相關人員的定期訓練、工作內容的明確劃分、職務輪調及職務代理人制度等。



圖六：資訊安全控管之範圍

資料來源：陳永裕，民 83

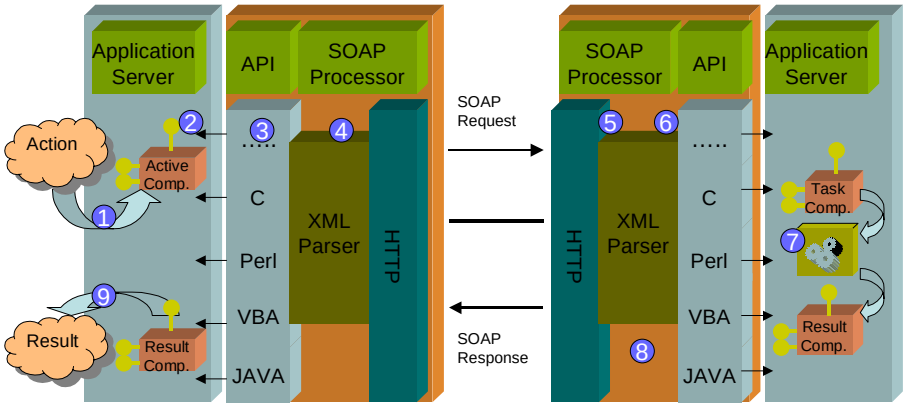
三 稽核資訊系統使用之主要科技

1. SOAP 規格〔40〕

為了以後討論方便，我們簡單介紹 SOAP 的架構與使用方法。

我們可以以圖四，SOAP Architecture 為例，說明 SOAP 站整體運作的步驟如下：

1. 程式產生一個需求（Request）動作。
2. 這個動作產生一個處理程序和需求介面。
3. 訊息被轉成 XML 格式且被送往 Web Server。
4. XML 解析器檢查 XML 文件之一慣性（consistency）且將之經由 HTTP 送往接收端。
5. 接收端的 XML 解析器利用 HTTP 和 XML 的標頭資訊（TAG）檢查所接受到訊息的合法性。
6. 訊息轉送到適當之應用程式且將 XML 訊息反組譯成為一般 Code。
7. 應用程式根據訊息客戶之需求內容（Request）執行工作。
8. 訊息以原先需求端發送訊息之相同模式經由 HTTP 將訊息回傳。
9. 原始需求動作接收到回傳之結果，完成 Request。

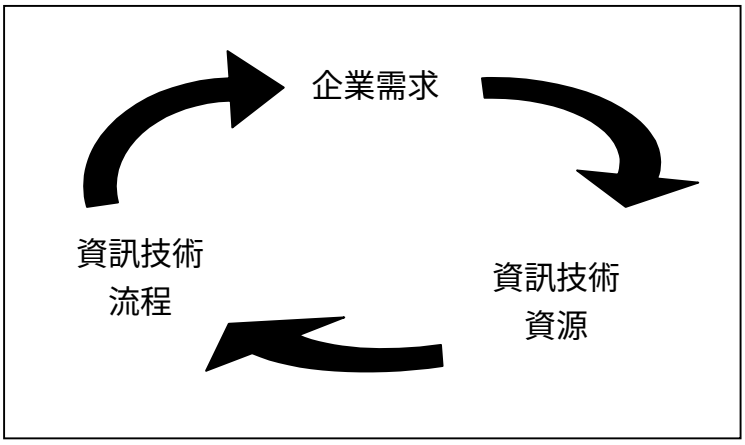


圖四　SOAP Architecture〔40〕

2.COBIT〔23〕

資訊系統稽核與控管協會（Information Systems Audit and Control Association, ISACA）在 1995 年發表「資訊及相關科技控管目的」（Control Objectives for Information and Related Technology），簡稱 COBIT。COBIT 是一套 IT 控管標準，係由全球各主要國家、政府機構與學術組織，廣泛蒐集資訊系統控管有關之標準及最佳化作業流程，經過國際性組織 ISACA 嚴謹地檢核後所訂定，除提供 ISACA 各國之會員及其他專業人員運用，亦適用於公、民營企業或政府單位等組織〔14〕。

COBIT 訂定在資訊環境下，內部控制的三個要素，分別為企業需求（Business Requirement）、資訊技術資源（IT Resources）及資訊技術流程（IT processes）等，此三要素間之交互相關性如圖五。COBIT 架構可提供管理當局、使用者、稽核人員等一個完整的內部控制架構，並能協助此三者達到以下功能：(1) 輔助管理當局在資訊投資和風險控制方面找出平衡點；(2) 幫助使用者在取得的產品與服務的安全和控制方面獲得保證；(3) 提供稽核人員相關工具與程序，以進行內部控制。



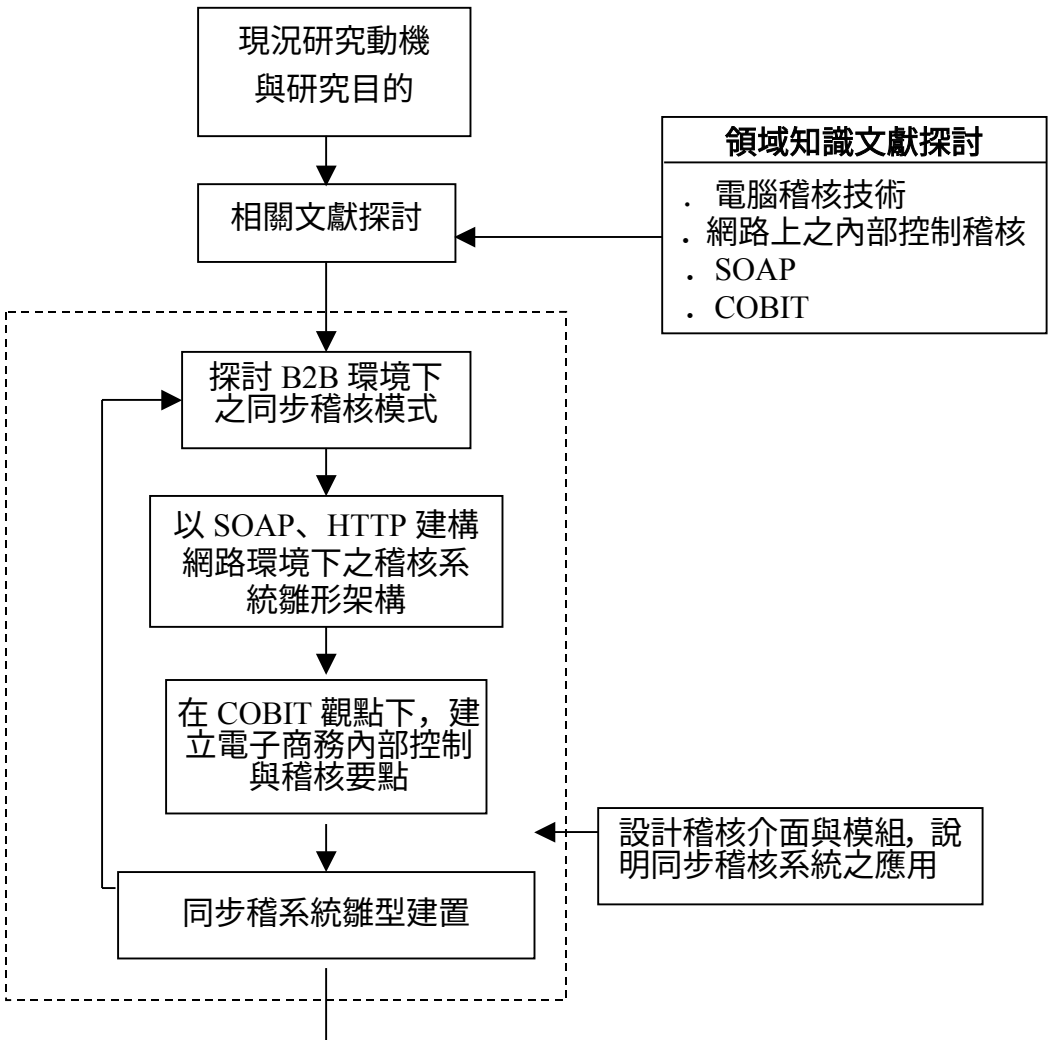
圖七　COBIT 內控架構示意圖

參、研究方法及進行步驟：

本計畫將分成二個部分來進行：首先整理電子商務與電腦審計之相關文獻，以及蒐集相關之資訊技術，深入探討在企業間（B2B）的電子商務環境下，如何以 ebXML、SOAP 等新技術，來加速同步稽核之可行性，從而決定稽核系統之架構與服務的內容。並實際以 XML、XBRL 等描述稽核元素及屬性，設計類別

圖及轉換為 DTD 規格，初步建構可應用於 B2B 電子商務之電腦輔助稽核系統雛型，此系統可以方便會計師隨時擷取，企業交易資料，進而執行預算、分析比對、統計等數量化分析之功能。第二部分則探討稽核資訊系統環境上安全管理與內部控制。因此，本文首先研究組織本身之安全需求、風險與內部控制目標，探討在電子商務環境下，企業之資訊安全與內部控制政策之變遷。其次，根據相關文獻探討與分析 COBIT 之架構，制定一套適用於受查企業 IS 系統的內部控制制度。此外並說明查核人員如何運用本研究之同步稽核系統與受查客戶之 IS 內部控制相整合，實際達成持續不斷的監控與抽查程序。最後設計同步稽核之模組範例，以驗證稽核資訊系統模式中所設立之安全機制與 IS 內部控制是否符合所需。

一、 研究流程：



圖八　研究流程

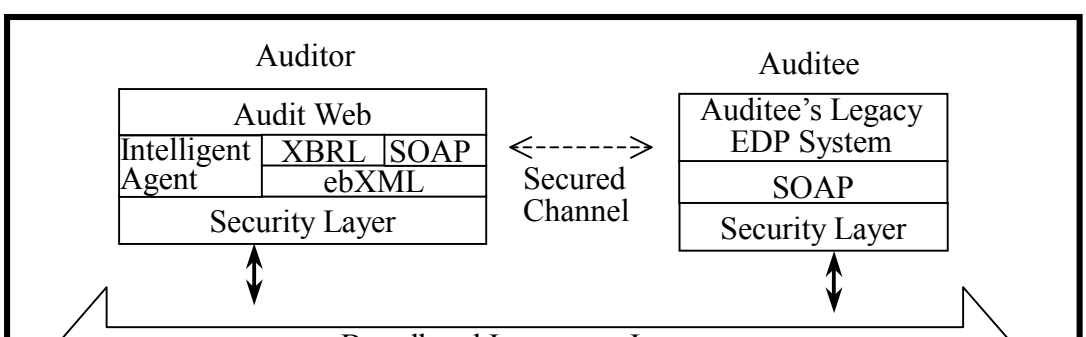
二、 研究步驟：

（一）文獻探討

搜集整理有關電腦審計與同步稽核技術之最新發展及資訊科技架構，其次參考本人國科會計畫實際訪談大型會計師事務所之結果，了解實務界對稽核資訊系統之需求，藉由蒐集相關文獻進行同步稽核模式下之網路風險管理與安全控制。依據吳琮璠（1999）認為安全的網路環境應包含下列要素：(1)安全且可靠的電子資料傳輸；(2)網路必須附有有效之資訊保護系統；(3)提供認證及確保隱密性之有效方法，以防止未授權者任意入侵網路上資料；(4)熟悉如何保護其系統和資料之網路使用者（吳琮璠，1999)。本計畫擬藉由對上述環境之了解，並藉由蒐集大量技術資料加以有系統的整理，以提供審計人員在資訊安全領域與 IS 內部控制之完整輪廓。

（二）建構符合目前 B2B 電子商務稽核所需之電腦輔助稽核系統雛形：

本計畫第一年主要是以新興之 SOAP 及 XML（含 ebXML、XBRL）等技術為基礎，配合概念圖形法（Conceptual Graph)、正規化描述法，以完成稽核資訊系統中相關元素的商業邏輯，再設計符合 XML 之 DTD 將整個工作規格建構（Structuring）起來，以方便事務所與受查客戶在網路上互享資料；至於稽核文件，其格式大都以欄位為組成方式，由於 XML 本身的功能能讓使用者可彈性地定義語義（Semantics）及標籤（Tag)，因此，本計畫以 XML 作為描述審計人員稽核文件的工具。本計畫之基本之架構圖，如圖九所示：

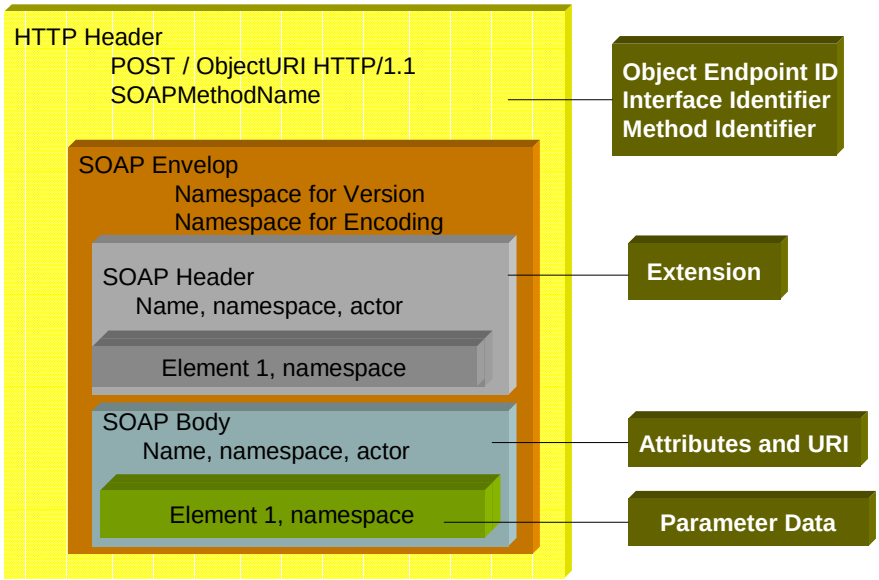


而建置此一稽核系統雛形架構之步驟，如下所示：

步驟一、對 SOAP 之技術，作深入之分析設計：SOAP 是由全球資訊網路協會（W3C）於 2000 年所提出的一個 XML-based 的分散式的系統網路環境。SOAP 標準，具有可使分散式

物件完全開放且在網路上傳遞。由於分散式物件可以達到客戶／伺服端之語言、作業系統獨立性，伺服端的高擴充性，通透性、自動化、以及物件結構性等革命性的優點。SOAP 的 Message Structure 如圖八所示，SOAP 的 Message 主要區分為三個部分：

1. SOAP Envelop.
2. SOAP Encoding Rule.



圖九　Message Structure of SOAP

圖十 Message Structure of SOAP

接著我們介紹如何在符合 SOAP 之規範來實作 Client 以及 Server 端之應用程式。Application Server 除了在 Server 端撰寫 Service 之外，還需要將 Service 以 WSDL 的格式 Publish 到 Internet，將此 WSDL 的 URI 註冊到 UDDI（Universal Description, Discovery and Integration）上。WSDL、UDDI、XML Schema 分別是 W3C 提出之標準，詳細的 Specification 請見〔48〕〔40〕。

為了介紹 SOAP 上的主從架構（Client-Server）程式的撰寫方式，我們用一個簡單的範例。並對此服務提出一個 WSDL 的服務描述檔如表一所示，針對於該服務提供之介面、參數以及提供服務之 URI 利用 WSDL 詳加描述於該檔案之中。

表一　WSDL of Sample Server

```
<?xml version='1.0' encoding='UTF-8' ?>
 <!-- Generated 08/08/01 by Microsoft SOAP Toolkit WSDL File Generator, Version 1.02.813.0
-->
<definitions name ='StockTrasnsationSamplev1' targetNamespace =
'http://tempuri.org/wsdl/'
        xmlns:wsdlns='http://tempuri.org/wsdl/'
        xmlns:typens='http://tempuri.org/type'
        xmlns:soap='http://schemas.xmlsoap.org/wsdl/soap/'
        xmlns:xsd='http://www.w3.org/2001/XMLSchema'
        xmlns:stk='http://schemas.microsoft.com/soap-toolkit/wsdl-extension'
        xmlns='http://schemas.xmlsoap.org/wsdl/'>
  <types>
    <schema targetNamespace='http://tempuri.org/type'
      xmlns='http://www.w3.org/2001/XMLSchema'
      xmlns:SOAP-ENC='http://schemas.xmlsoap.org/soap/encoding/'
      xmlns:wsdl='http://schemas.xmlsoap.org/wsdl/'
```

```
        elementFormDefault='qualified'>
    </schema>
</types>
<message name='SampleServer.add'>
    <part name='n1' type='xsd:int'/>
    <part name='n2' type='xsd:int'/>
</message>
<message name='SampleServer.addResponse'>
    <part name='Result' type='xsd:String'/>
</message>
<portType name='SampleServerSoapPort'>
    <operation name='add' parameterOrder='n1 n2'>
        <input message='wsdlns:SampleServer.add' />
        <output message='wsdlns:SampleServer.addResponse' />
    </operation>
</portType>
<binding name='SampleServerSoapBinding' type='wsdlns:SampleServerSoapPort' >
    <stk:binding preferredEncoding='UTF-8'/>
    <soap:binding style='rpc' transport='http://schemas.xmlsoap.org/soap/http' />
    <operation name='add' >
        <soap:operation soapAction='http://tempuri.org/action/SampleServer.add' />
        <input>
            <soap:body use='encoded' namespace='http://tempuri.org/message/'
                encodingStyle='http://schemas.xmlsoap.org/soap/encoding/' />
        </input>
        <output>
            <soap:body use='encoded' namespace='http://tempuri.org/message/'
                encodingStyle='http://schemas.xmlsoap.org/soap/encoding/' />
        </output>
    </operation>
</binding>
<service name='SampleServer' >
    <port name='SampleServerSoapPort' binding='wsdlns:SampleServerSoapBinding' >
        <soap:address location='http://localhost:8080/soap/servlet/rpcrouter' />
```

```
    </port>
  </service>
</definitions>
```

步驟二、建構一可應用於企業間電子商務活動之稽核資訊系統架構模型：由於企業對企業間（B2B）的電子商務活動較具結構化，且有既定的合作關係為基礎，其對資訊科技之應用也較為先進。因此，本計畫乃擷取上述文獻與技術之概念，針對稽核流程發展同步之稽核資訊系統架構，其內容包括 UML 分析設計、SOAP 實作、應用 ebXML 彈性地定義、語義及標籤以及與 HTTP 相配合，尤其在 Information Model 與 ebXML 部分特別重要，因為整合不同資料結構與系統架構之資訊系統，需有一套架構完整與標準化的交換機制支援。藉由系統測試與相關研究比較，再回顧修正 B2B 電子商務之稽核架構模型。

步驟三、設計稽核介面之間的對應關係與稽核流程：本研究以 SOAP 為基礎平台，以 UML 作為分析設計之工具，建構本系統 XML-based 資料模型之類別圖，並轉換為 DTD 規格。本計畫將初步設計執行同步稽核所需用的 ebXML DTD 與稽核文件之間的對應關係與稽核流程，例如現金流量之審核、物流控制等。另外設計同步監控模組（Continuous Monitoring Module）監督電子商務日常的作業，遇有異常狀況，則產生例外報告給稽核人員。同步監控
模組主要的應用為：(1) 高風險交易的監督。(2) 產生例外報告。(3) 偵測詐欺。(4) 監督存貨趨勢與週轉率。(5) 監督電腦處理之功能，如機密檔案的存取與密碼的使用等。並製作實例反覆修改驗證及輔助說明，再以 Web 系統來執行資料交換的作業，如圖十所示，藉由已定義之 EDI 標準訊息及 XML-based 標準文件，說明加值網路或 Web 交換電子商務異動之資料。

本計畫以 ebXML 標準來設計相關的稽核元素，其主要之理由如下：

1. **與 Internet 結合：**現今電子商務、資料交換及物流系統等各領域都是架構在網際網路上，由於 XML 文件文身直接支援 Web 的通訊協定且為網路上的資料傳輸提供串列化（serialized）的標準格式。
2. **文件可讀性高：**ebXML 文件內容都是文字型態，可在文件中直接宣告屬於何種編寫、格式語法、文件結構、元素的屬性等資料溝通單純化，不若現存的資料交換機制都是二進位格式，必須再執行轉換（Transform）的步驟。
3. **文件組織有彈性：**由於 ebXML 本身可定義有語意（Semantics）標籤，標籤的內容也很有彈性不限於純文字模式所以在描述事物可更為詳細，此外對資料結構化的描述也是 ebXML 的特色。
4. **剖析（Parse）簡單：**由於 ebXML 文件的組織簡潔、嚴謹，語法清楚，

故剖析 ebXML 文件較為簡單。

XBRL（eXtensible Business Reporting Language）是以 ebXML 為基礎發展的語言，它可讓用者 SEC 的網路上下載企業之財務報表，並可立即轉換為 Excel 檔，本研究亦將探討 XBRL 之發展及趨勢。

（三）B2B 環境下電腦稽核與安全控制之觀念性架構：

網路交易時代趨勢，資訊安全威脅如影隨形，依照歐美國家發展經驗分析其原因可歸納二個來源：

1. 來自內部威脅：包括承包商及內部員工，員工又分人為疏忽及犯錯、心懷怨恨及不誠實有意舞弊，而內部威脅佔 80%。
2. 來自外界的威脅：包括 Internet 漫遊者、產業間諜、競爭對手及外國政府、地下組織等，拜電子商務之賜，財務欺騙及資訊財產的竊取越來越容易，此種威脅約佔 20%。

由此可知，電腦資訊安全絕不是單純的技術問題，許多存在於現實狀況中之安全漏洞，其實是源自內部管理層面需求不明確所造成，因此在考慮組織內的資訊安全架構時，內部稽核尤其是電腦稽核亦是一個重要的議題。

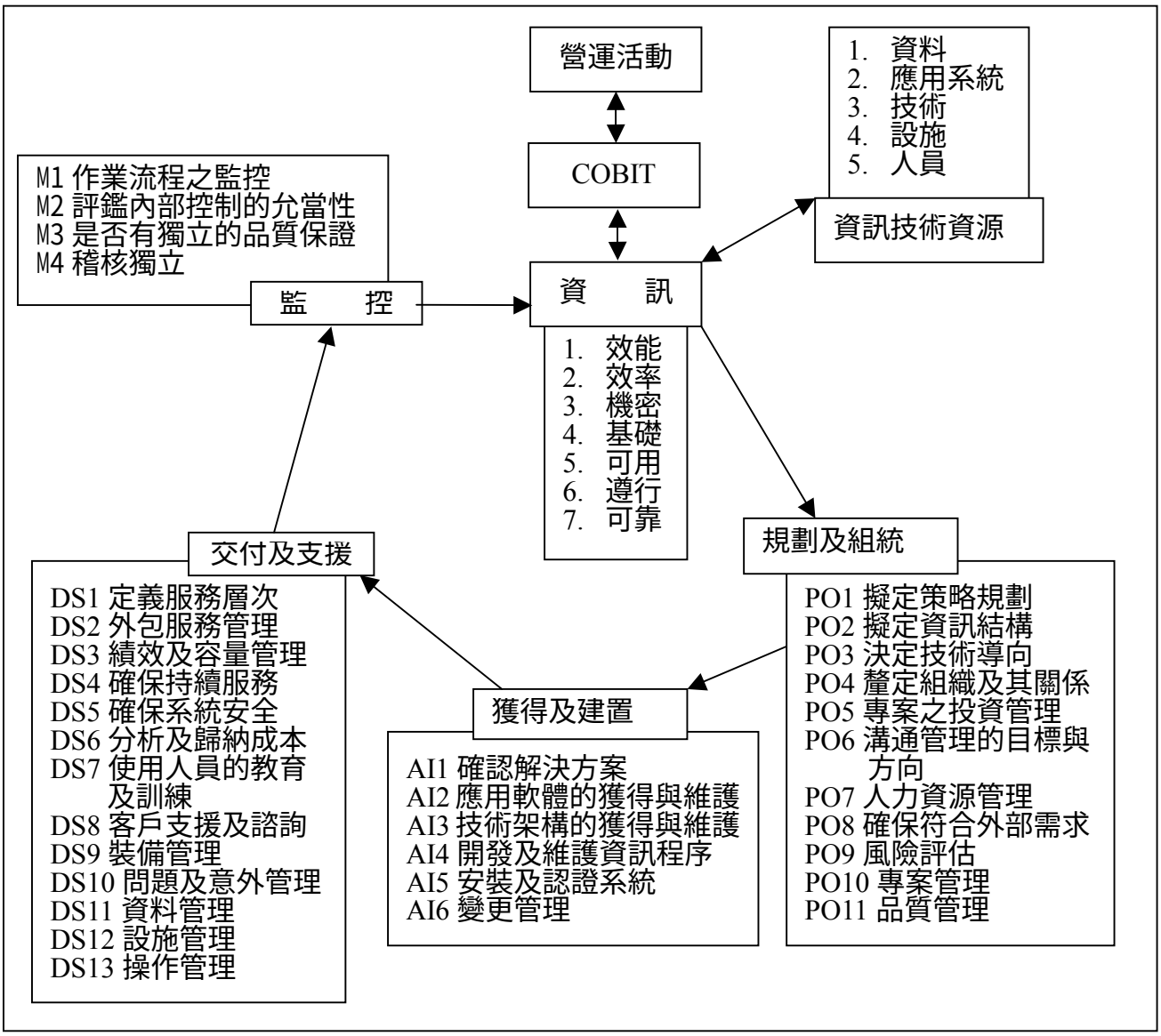
因此，本年度計畫除探討上述資訊系統之風險與安全之防護技術，並將與第一年同步稽核架構之 SOAP, HTTP 以及 ebXML 等技術之安全架構加以檢視外，並由稽核人員或制度面之角度切入，來探究組織可能面臨的資訊安全威脅，以達到交易安全與作業控管上之全面性需求。

（四）在 COBIT 觀點下，建立與電子商務政策與內部控制稽核要點：

COBIT 係由電腦稽核協會（Information System Audit and Control Association）參考全球不同國家、政府機構與標準制定單位，包括美國 COSO、英國 Cadbury、加拿大 COCO 之內控模式，以及「專注於控管模式」之英國安全行為守則（Security Code of Conduct Department of Trade and Industry）及美國安全手冊（Security Hand book-National Institute of Standards and Technology）等，有關資訊系統控管標準及最佳作業實例而訂定，並將控管與營運目標緊密聯結。本計畫擬參考 COBIT 架構

下之資訊技術安全控管之內容，以檢視同步稽核資訊系統內之安全控管與風險問題，並提出具體建議。COBIT 資訊技術安全控管之整體

架構如下圖所示：



圖十一 COBIT 資訊技術安全控管之整體架構

肆、研究貢獻

（一）**藉以確立一個同步稽核資訊系統架構及其導入程序：**本計畫以 SOAP 為基底配合 HTTP 之機制，設計一套適用於 B2B 電子商務環境下的稽核程序。此稽核架構對會計師而言不僅是資料的取得與交換而已，還可以使會計師將不再受制於受查客戶異質環境之影響，且由於 End-User Computer 的發展，會計師可設計更具功能的通用電腦審計軟體，具有提高稽核效率、縮短稽核時間、改善稽核品質等功能，有助於企業競爭能力的提昇。

（二）**在學術領域上本計畫可以提供審計人員如何因應電子商務環境時的轉變：**電子商務可以說是世紀末前的重要顯學，有越來越多的研究紛紛指出各種產業在面對電子商務這樣一個新的環境時，所發生的衝擊與轉變。因此本計畫透過會計師事務所電腦稽核的現況瞭解，尋找出部分脈絡，提供後續研究者在進行同步電腦稽核研究時的部分啟發。

（三）**在實務領域上的貢獻為提供一個支援會計師事務所既有資訊系統、符合電子商務特性且充分整合的系統規格及藍圖：**本計畫透過對目前電子商務環境上的攸關資訊科技進行詳細且深入的了解，進而建置本系統的實驗平台，驗證這些資訊科技間的關係及相容性，且將這樣的經驗提供給會計師界，作為其執行系統規劃或開發時的重要參考。

（四）**首度以分散式物件規模中之 SOAP 為基底，導入稽核資訊系統之中：**本計畫首先設計以 SOAP 為基底之稽核資訊系統開發時所需之基本介面與標準資料之準則，可作為有意發展分散式稽核資訊系統者之參考。使用本計畫所設計之稽核資訊系統不僅能使審計人員減少對受查客戶資訊部門的依賴性，順利擷取與分析資料，且能更進一步達成同步稽核之高階電腦查核目標。

（五）**提出對受查企業 IS 系統之安全設計與整體性的內部控制方針：**由於電子商務環境下之電腦稽核乃是運用電腦與通訊科技傳輸技術，對安全需求措施亦較封閉式或專屬網路之要求更為嚴苛，因此對系統開發、維護、更新之管理亦較為殷切為達到開放系統下安全的需求，本計畫擬參考資訊技術與 COBIT 架構，對安全控制設計及緊急應變措施等內部機制提出具體規劃及實施方針，以提高系統之可用性。

（六）**可積極加強專業人員的訓練，提昇參與人員之專業知識：**藉由本計畫建立相關人員對稽核資訊系統應用之認識以及正確的 IS 內部控制及稽核風險觀念，以期達到持續性的風險管理、控制及監督過程的有效性，進而提昇查核之品質。

伍、參考文獻

一、中文部分

1.王惠真，“ 中小企業會計資訊系統引進程序之研究 ”，國立台灣大會計研究所碩士論文，民國 86 年 6 月。

2.王瑞之，“ 物件導向會計資訊系統之設計 “，國立交通大學資訊管理研究所碩士論文，民國 86 年 2 月。

3.李美慧，“ 利用資訊技術協助金融機構之管理稽核 ”，國立成功大學會計學研究所未出版碩士論文，民國 86 年 6 月。
4.余千智、周濟群，“ 電子商務環境中計及審計作業之流程模式 ”，中山管理評論，第五卷，第四期，民國 86 年。
5.吳琮璠、謝清佳和著，“ 資訊管理－理論與實務 ”，民國 81 年 1 月。
6.吳琮璠，“ 會計資訊系統與電腦審計 ”，民國 87 年，智勝出版。
7.徐義雄譯，“ 金融機構經營與管理 ”，美國金融機構研究中心編譯，台北市金融機構與幼獅文化事業公司合作出版，民國 69 年 9 月出版。
8.耿晴，“ 跨出電腦審計一小步－突破傳統稽核一大步 ”，會計研究月刊，第 54 期，民國 79 年 3 月。
9.翁霓、吳典明譯，“ 商業金融機構的管理政策 ”，幼獅文化事業公司，民國 80 年 4 月。
10.陳章正，“ 金融機構營業單位之電腦查核 ”，台北銀月刊，第 18 卷，頁 21-28。
11.葉誌崇，“ EDP 審計之研究 ”，國科會計畫研究報告，民國 74 年 7 月。
12.林鳳儀，“ 以 CORBA 為基底輔助會計師稽核訊系統之架構 ”，國立交通大學經營管理研究所未出版博士論文，民國 89 年 7 月。
13.周濟群，“ 連續性審計理論分析與系統技術探討---以物件式雛型系統為例 ”，國立政治大學會計研究所未出版博士論文，民國 89 年 7 月。
14.樊國楨，COBIT 資訊及其相關技術之控管目標與應用簡介，內部稽核會訊 29 期，88 年 10 月。

二、英文部分

15.AICPA and Canadian Institute of Chartered Accountants（CICA）, Continuous Auditing 1999.
16.AICPA and CICA. Electronic Commerce Assurance Services Task Force. *WebTrust Principles and Criteria for Business-Consumer Electronic Commerce*, Feb. 1999. Ver. 1.0.
17.AICPA and CICA. SysTrust$^{SM/TM}$ Principles and Criteria for Systems Reliability. July 1999. Ver. 1.0.
18.American Institute of Certified Public Accountant, “Auditing in Common Computer Environments”, AICPA, New York, 1995.
19.American Institute of Certified Public Accountant, “Auditing with Computers”, AICPA, New York, 1994.
20.B. E. Cushing and M. B. Romney, “Accounting Information Systems-A

Comprehensive Approach", 5th ed. Addison-Wesley. 1990.

21. Bruce Schneier, "Applied Cryptography – Protocols, Algorithms, and Source Code in C", John Wiley and Sons Inc., New York, 1996.
22. C. Zoladz, "Auditing in an Integrated EDI Environment", *IS Audit & Control Journal*, Vol. II, pp. 36-40, 1994.
23. "COBIT-Audit Guidelines" 2nd Edition, Information System Audit and Control Foundation, April, 1998.
24. D. R. Carmichael, J. H. Willingham, and C. A. Schaller, "Auditing Concepts and Methods-A Guide to Current Theory and Practice", McGraw-Hill, 1996, 6th ed.
25. Dave Coderre, "CAATs and Other Beasts for Auditors", *The Internal Auditor*, Oct. 1997, pp. 18-20.
26. Doug Pirie & Don Sheehy, "Electronic Commerce", *CA Magazine*, Jun/ Jul 1996, pp.45-50.
27. Deron Liang, Fengyi Lin, Soushan Wu "Electronically Auditing EDP Systems – With the Support of Emerging Information Technologies", *International Journal of Accounting Information System*, 2001.
28. Fengyi Lin, Deron Liang, Soushan Wu and Ray M. Yang, "An Integrated Auditing Architecture for Internet and Information system Design under a CORBA Environment", *Review of Accounting Information Systems*, Vol. 4 No.1, Winter 2000.
29. Groomer, S.M. and U.S. Murthy, "Continuous Auditing of Database Applications: An Embedded Audit Module Approach", *Journal of Information Systems*, Spring 1989.
30. J. I. Cash, A. D. Bailey, Jr. and A. B. Whinston, "A survey of techniques for auditing EDP-based accounting information systems", Accounting Review, Vol. III, No. 4, pp. 813-832, Oct. 1977.
31. J.V. Hansen, and N. C. Hill, "Control and Audit of Electronic Data Interchange", *MIS Quarterly*, pp. 403-414, Dec 1989.
32. Jim Rumbaugh, "The Unified Modeling Language: Reference Manual", Addison Wesley, 1999.
33. L. C. Mohrweise, "Usage of Concurrent EDP Audit Tools", *The EDP Auditor Journal*, III, 49-54, 1988.
34. Nunamaker, J.F., "Build and Learn, Evaluate and Learn", *Information*, 1992. pp. 1-5

35.Office of the Comptroller of the Currency, Internet Banking, Comptroller's Handbook, October 1999.

36.R. Watson, "The Use of Microcomputers in the Audit Environment", *The EDP Auditor Journal*, Volume I, pp. 31-42, 1988.

37.Ravi Kalakota & Andrew B. Whinston, "Electronic Commerce; A Manager's Guide", Addision Wesley, 1997.

38.Scott-Morton, M.S., "The State of the Art of Research", *The Information Systems Research*, Poston: Harvard Business School Press, 1984. pp. 13-41.

39.Sofia Giannakoudi, "Internet Banking: The Digital Voyage of Banking and Money in Cyberpace", *Information & Communications Technology* Low, Vol.8, No.3, 1999.

40.Simple Object Access Protocol (SOAP) 1.1 , http://www.w3.org/TR/SOAP/

41.SSI Ltd., et at., "General Ledger Facility", OMG DTC Document finance/98-07-02, 1998.

42.T. E. Gibbs and R. G. Schroeder, "External Auditor Criteria for Evaluating Internal Audit Departments", *The Internal Auditor*, pp. 34-42. Dec. 1980.

43.The Common Object Request Broker: Architecture and Specification, Revision 2.0, Jul. 1995, http://www.omg.org/CORBA/corbiiop.htm.

44.T. W. Lin, and D. C. H. Yang, "The use of microcomputers in auditing- a survey", *EDP Auditor Journal*, Vol.4, pp. 73-80, 1990.

45.V. Zwass, "Electronic Commerce: Structures and Issues", International Journal of Electronic Commerec, Fall 1996.

46.Vasarhelyi, M. A. & Halper, F. B., The Continuous Audit System: A UNIX-Based Auditing Tool, *The EDP Auditor Journal*, 1991, pp. 85-91.

47.UDDI White Paper, http://uddi.org

48.W3C, "XML Stylesheet Language Transformation Specification", http://www.w3.org/TR/xslt

49.XML Schema Part 0: Primer , http://www.w3.org/TR/xmlschema-0/

50.Yu, C. C., H. C. Yu and C. C. Chou, The Impacts of Electronic Commerce on Auditing Practices: An Auditing Process Model for Evidence Collection and Validation, *the International Journal of Intelligent System in Accounting, Finance and Management*, 2000.