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

網路服務（Web Services）環境下之網路稽核安全架構與風險控管政策之研究

A Study on Web Application Security Framework and Risk Control Policy Under Web Services Environment

計畫類別：▓ 個別型計畫　　□ 整合型計畫
計畫編號：NSC　92－2416－H　263　－001　　－　　－
執行期間：　　92 年　08　月 01 日至　93　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 白東岳 郭明泉

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　　93　年　07　　月　　31　　日

摘　　要

隨著科技資訊的進步，投資人對會計師及時揭露財務資訊的需求與防範舞弊等功能的要求也愈高。網路服務（Web Services）技術的興起，解決了分散式環境下異質系統之溝通問題，使得會計師事務所開發其與受查客戶間的同步稽核資訊系統，以提昇稽核品質的概念得已實現。然而，在開放式的網路系統上，受查企業之機密資訊極易直接暴露於公眾網路上，且 SOAP 的安全機制僅限於點對點的安全性，對於來自網路上的威脅仍難以防禦，且財務資料一旦遭受侵害，損失甚鉅。因此，審計人員在查核財務報表時，如何在安全的環境下運用新興科技，以持續地覆核與監控受查企業，乃成為一項重要之議題。本計畫研究之主要目的乃針對目前網路服務環境之網路稽核安全架構，開發網路服務在 SOAP 平台上之監控模組，以監督跨企業之電子交易或入侵。此外，並對於風險控管理政策作初步的探討。

關鍵詞：網路服務、會計資訊系統、電腦輔助稽核技術、同步稽核、資訊安全

English Abstracts

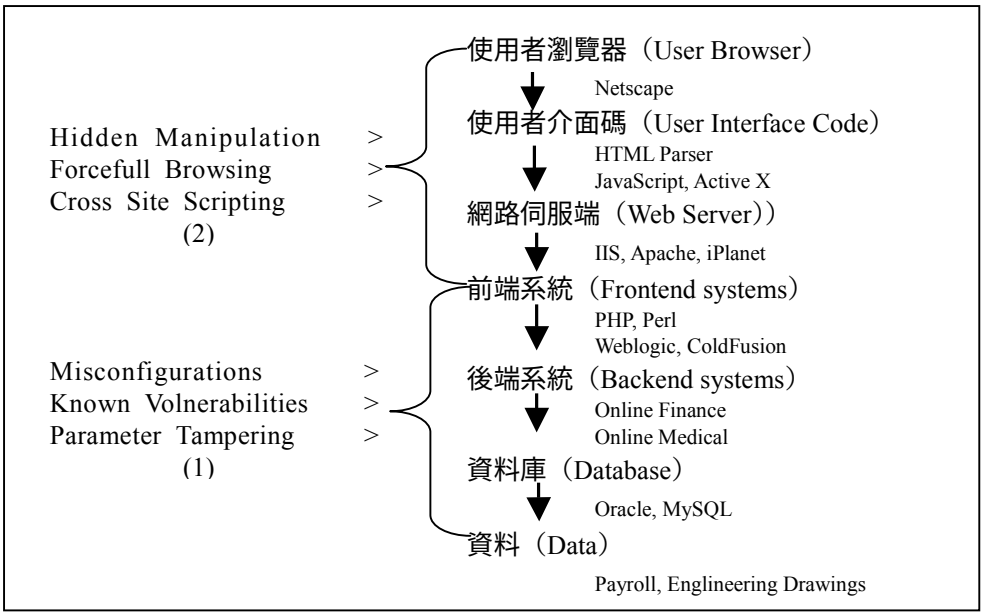
As the increasing dependency on information technologies, auditors are required to disclose the information of financial statements at continuous basis in order to prevent Internet fraud effectively. Web services resolve the communication problem so that the interoperability issues of disparity EDP system can be addressed. This trend has leaded the continuous auditing concept between CPAs and its auditees become possible. However, companies' confidential financial information is easily exposed on public websites when it utilizes Web Services. Under the Web Services, SOAP (simple object access protocol) contains limited security mechanisms in order to protect information's confidentiality, integrity and availability. Therefore, we would like to study on Web application security framework and develop continuous review modules over the SOAP in order to monitor intercompany's transactions and network threats. In addition, past literatures have pay attentions to firewalls, intrusion detection systems (IDS) and other security products. However, it is also very important to address information security form management perspectives and identify the security management to higher-risk area.

Keywords: Web Services, Accounting Information Systems, Computer-assisted Auditing Techniques (CAATs), Continuous Audit, Information Security

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 Gartner Group 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至 2004 年產值已高達美金 7 兆 3 千億，約佔全球整體經濟的 6.9％，而危害資訊安全的風險也隨之增加。2001 年中 CERT(Computer Emergency Response Team)共處理了 52,658 件安全事件（security incidents），比起 2000 年的 21,756 足足多了一倍。且至 2001 年止，CERT 所處理的安全事件次數，已經連續三年呈現每年倍增的狀況。網路上的攻擊事件的層出不窮，連專家們也體驗到安全事件本質的改變。在 Internet 蓬勃發展之前，一般使用者最常受到的攻擊是電腦病毒（computer virus），此種病毒乃以破壞使用者的個人電腦為目的。其破壞層面如圖一之（1）所示，始自前端系統、後端系統至資料庫，病毒發病的情況包括前、後端系統的入侵、摧毀檔案系統、電腦的行為異常、速度變慢或當機等。

但隨著近年網路服務（Web Services）的興起[27][31][33]，取代了現存的分散式運算系統，網路服務預設的網路通訊協定是 HTTP 協定，此技術可以應用在許多方面，例如：網路服務可以在桌上型電腦和可攜式設備上執行，存取網際網路上的應用程式，像是訂位系統和訂單追蹤系統。網路服務也可以應用在企業對企業（B2B）的整合，連接同一個供應鏈上不同組織執行的應用程式。另外，網路服務也可以解決企業系統整合（EAI）的各種問題，將單一組織的多個應用程式與防火牆內外的其它應用程式作連結。因此使用方式也從過去以資料為主（data-centric），變成了以人與人互動為主（people-centric）的通訊管道。另一方面，由於公司內員工電腦也有連接網際網路，使得這些個人電腦成為公司內部網路安全上最弱的一環，也是入侵者的主要目標。一旦攻陷某台員工的電腦，即可進入整個內部網路，繞過公司所架構的安全機制。在新的網路服務（Web Services）中的入侵事件除過去的前、後端系統及資料庫外，更擴及至如圖一中（2）之使用者瀏覽器至網路伺服端，入侵的目的除了破壞外，尚有資料的竊取、信用的盜用、或資源的使用等，因此網路服務上安全性的考慮也必須較以往更為全方位[14]。



圖一、網路服務下之入侵狀況（Stasiak, 2002）

對於會計師的稽核業務而言，許多以 web-based 為基礎的電子商務受查企業，將其營運得重點放在數位化的財務交易及資產控制程序，因為進入網路經濟時代，除了帶動全球化、作業流程虛擬化、技術演進等優勢外，也產生了許多潛在的風險與威脅。且而隨著 e-business 頗客的快速成長與發展現今的電腦犯罪，一但發生所造成的損失都十分重大，因此會計師在查核財務報表時更應將查核的重點放在顧客交易程序的改變以及資產控制的方法（Greenstein M. and Ray A., 2002），並重新思考及改造現行的管理架構與服務內涵。

大型的會計師事務所及其所設立的管理諮詢公司，近年來開始加入安全服務的行列，如 Pricewater Coopers（PwC）的全球風險管理業務（GRMS），不僅提供週期性的安全評估及基礎建設，且進一步提供商業過程的安全與控制，如： 1.安全的威脅及弱點的評估服務。2. 安全整合服務。3. 管理安全的解決（MSS）。4. 防電腦犯罪的服務。5. e-Trusted 的認證服務等。Accenture 管理諮詢服務，則強調企業各類型的資訊安全諮詢、安全構造設計、執行、及管理服務等[1]。

網路服務（Web Services）技術的興起，解決了分散式環境下異質系統之溝通問題，使得會計師事務所開發其與受查客戶間的同步稽核資訊系統，以提昇稽核品質的概念得已實現[7][8][10][22]。然而，在開放式的網路系統上，受查企業之機密資訊極易直接暴露於公眾網路上，且 SOAP 的安全機制僅限於點對點的安全性，對於來自網路上的威脅仍難以防禦，且財務資料一旦遭受侵害，損失甚鉅。因此，審計人員在查核財務報表時，如何在安全的環境下運用新興科技，以持續地覆核與監控受查企業，乃成為一項重要之議題。因此本計畫的第一個目的即探討在 Web Services 環境下，新型的電腦駭客的攻擊型態對同步稽核模式下資訊設施的影響及其因應的稽核安全模式，以建構出適用於會計

稽核業務和符合網路服務特性的資訊安全系統架構，做為會計師業發展電腦稽核工作之參考。

有鑑於資訊安全技術是確保組織資訊安全重要的一環，在稽核上除了確保資訊安全相關技術的應用，如對於資料的加密保護、防火牆的技術、電腦病毒學及電子商的安全機制等的運用外，更應重視資訊安全的管理層面[12、13]。再者，受限於資訊犯罪的手法實在太多又太新，因此要資訊單位或安全部門獨力承擔實無可能。相形之下，「管理制度」就成為協助「人」的工具，透過健全的資訊安全制度，不僅可以大幅降低不利因素，亦可達到損失最小的目的。因此本計畫第二個目的即由政策上的管理與實體上的控制，來探討受查企業的資訊安全政策，以徹底瞭解組織資訊安全所面臨威脅的風險加以分析，，建立網路服務環境下，應用於會計師稽核之資訊安全風險控管機構[7、8]。

一、研究動機

洪振添與余麗玲（民國九十年）認為認為ｅ世代審計專業服務之發展方向包括：(1)網路認證服務（Web Trust）(2)高度電腦化流程控制與安全控管服務(3)企業流程暨內部控制制度之設計與複核服務(4)內部稽核服務(5)風險管理等，由此可見安全控管已成為 e 世代的重要議題。

Internet Week 網路民調顯示，阻礙人們上網消費的原因中，排名第二的是 EC 交易平台的系統安全 (system security)，資訊安全專家相信網路上經常出現的駭客攻擊事件（Internet attack）是主要因素。很多文獻的解決方法是採用安全的網路技術，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。然而隨著網路服務的出現改變了以往分散式系統間的整合方式，且由於網路結構建置速度很快，因此若無一套有效的安全防禦機制，則病毒的入侵與傳播就更為容易。資訊科技的發展，使得企業的資訊系統較以往更為複雜，也改變了會計師服務的內容，因此會計師在建構稽核受查客戶的電腦輔助稽核資訊系統時，網路安全的重要性更不言而喻。

我們在民 91 年曾提出一套以 SOAP 及 ebXML 技術以建構 B2B 電子商務下之同步稽核雛型[10]，使會計師在執行審計工作時，可不必受限於受查企業不同的應用軟體、平台之限制而能透過適當授權，取得客戶資訊，此項研究之績效亦已陳述於我們所提交之研究報告中。而在建構這套系統架構雛型的過程中，我們發現網路上曾出不窮的攻擊方式，亦嚴重影響到會計師運用電腦稽核財務報表的可行性及可靠性[11、19、20]。因此，本研究第一年之計畫擬研究新型網路攻擊的型態，並延續過去同步稽核雛型的基礎，設計一套具彈性與擴充性的網路稽核安全架構，以補強現行 Web Services 環境下安全性之不足，並嘗試在此安全雛型中加入稽核模組，以支援會計師業發展電腦審計工作的參考。

鑑於資訊科技的迅速發展，資訊安全的重要性也日漸提昇。現今資訊安全所強調的

範圍多數偏重資訊安全的技術層面，然而實際上，危害資訊安全的事件，反而以人為因素的影響最大，因此對於資訊安全的有效管理，才是確保資訊安全最好的方式。現今各國或組織對於資訊安全管理訂定相當多的規範，如 COBIT、BS7799、ISO17799、VISA 等[7、8、16、27]，這些制度都訂有複雜的資訊安全應用與稽核的標準，可用來對組織之資訊安全作業實施檢討評估，提供組織在資訊安全防範於未然的工作上。

國際電腦稽核協會 ISACA（1998）〔16〕提出對資訊系統內部安全控制的 COBIT 資訊技術架構。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、計劃之了解與執行。

BS7799[7][8]其內容與實施步驟機乎包含了資訊安全所有的面向, 同時該規範亦已成為國際標準組織所通過之標準 ISO17799，並廣為各國據以參考推廣使用。VISA[27]則被廣泛地應用於 B2C 的網路商業中。本計劃擬深入探對這些安全控制之內涵，並檢討這些規範，能否有效制止 Web Services 環境下所衍生的新型入侵狀況，即研究資訊安全可能發生的風險與政策，並對網路安全作風險的辨認與評估，從而建立一套資訊安全風險控管政策，由管理面來改善資訊安全上的缺失，有效管理資訊安全。

二、研究重要性

IDC 估計目前在 B2B 網際網路安全軟體上的花費約 35 億美元，至 2004 年預期會提升到 89 億美元。為了加強網際網路的安全性，Cisco Systems、IBM、Intel、Nortel Networks 和 Symantec 在 2000 年 1 月共同成立了資訊技術-資訊分享和分析中心 (IT-ISAC) [https://www.it-isac.org/]。其主要目的便是為了實踐網路的安全性，從而促進 B2B 商業的成長。

隨著電子商務的快速成長，會計師事務所的查核人員在執行審計工作時，開發其與受查客戶間的稽核資訊系統，以提升審計效率已不再是遙不可及之事。依據 Dalton, Hill and Ramsey（1994）之研究指出，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的功能愈來愈高，會計師唯有強化同步稽核技術，才能減少在電子商務環境下的審計風險。Glover

& Romney（1998）亦認為電子商務環境下的重要工作乃持續性的覆核與監控。由於網路稽核的安全與風險不同於傳統的稽核服務，而安全與風險又是會計師與受查客戶，是否應用網路稽核資訊系統的主要考量因素，運用 Web Services 所建構的稽核架構，雖可解決異質平台之溝道通問題，但 Web Service 上的安全機制不足，只能解決點對點的安全性。因此引發本文擬探究網路稽核之安全與風險問題，並研究如何在多點訊息路徑上，維護資訊安全內容。此外為加強組織之風險管理與安全政策，乃比較各國及組織對於資訊管理之規範，設計一套網路資訊系統安全之風險管理與步驟，進而擬定一套可支援網路稽核安全的風險控管政策。茲將本計畫之重要性列示如下：

1. **利用網路服務的資訊技術重新檢視同步稽核之功能**：以系統性的方法對 Web Services 之功能進行彙整，以修正過去同步稽核的雛型架構[21][22]。本階段整合電腦審計的相關技術 Web Services 中的 SOAP、WSDL 和 UDDI、XML、Web Security 等。
2. **發展出以 Web Services 為基礎之網路稽核安全系統，以有效保障財務資訊的傳輸**：在 Web Services 的環境下，所有會計物件可以透過 Web Services 跨越各種工作平台及網路通訊協定互相傳遞，克服了過去會計師在執行電腦審計時，受查客戶異質 EDP 系統之限制。但因網路服務（Web Services）在開放式的系統上暴露其程式和資料的存取，再加上複雜的稽核系統，其資料的存取與轉換會涉及到多個服務，而這些服務可被組合成更大的作業流程。因此，Web Services 環境下的稽核系統需要一個完整對話的端對端安全模型，以保障財務機密資訊的傳輸。
3. **探討 e 世代網路服務中，會計師簽證業務的發展方向**：在會計師面臨 e 世代的業務內容時，應具備何種知識與技能才能因應。本計畫針對目前 PwC 提出的全球性風險管理業務（GRMS）以及 Accenture 的安全架構業務深入研究，以提供後續會計師發展資訊安全簽證業務之參考。
4. **探討如何在多點訊息路徑上維護安全內容，並設置及時監控受查客戶之交易，以降低審計風險**：網路服務是一個新興的媒體，可供一個會計師稽核不同受查客戶資訊系統之平台，並且充分和企業內部的既有系統或作業流程緊密結合。在安全上除了強化 HTTP 的安全機制外，擬開發內嵌式監督稽核模組（Continuous Monitoring Modules）來截取高風險區的資料或偵知入侵駭客之攻擊，當某些違規交易或異常狀況發生時，系統自動產生例外報告（Exception Report），亦可針對某些重要交易製作交易追蹤（Transaction Tagging）俾益檢核交易控制的程序。本計畫運用 plug-and-play 的方式在適當的電子商務交易控制點上，設計與插入會計師專屬之安全稽核模組，從而偵知舞弊及入侵事件，強化稽核作業處理的效率，以降低查核風險提昇服務品質。
5. **對於目前已有的資訊安全管理標準加以比較分類，作為制訂資訊安全風險管理政策**

之參考：過去的資訊安全管理標準多強調前端的資訊安全政策管理，如圖一（1）的部分，但自網路服務興起後，新的網路攻擊層出不窮且影響層面擴增至全方位，如圖一(2)。為探討網路服務下的安全管理標準，因此本計畫擬深入研究下述之資訊安全規範與政策：1.「資訊及相關科技控管目的」(COBIT, Control Objectives for Information and Related Technology)；2.英國資訊安全管理標準－BS7799；3.ISO17799 及 4.VISA；5.與稽核安全相關的領域知識等。以系統化的方法進行彙整，並加入新型網路服務環境下的安全考量，經由此資料的蒐集，可作為後續研究的背景參考。

6.在管理制度上，提出對同步稽核系統之安全控制及方針，可供資訊系統在規劃建置時之依循：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式的傳輸系統，因此其安全需求更加重要。本計畫擬由過去相關之同步稽核與電腦審計研究之經驗，提出有關網路服務環境下之安全需求與風險管理政策，作為會計師未來簽證業務之參考。

7.提供高附加價值的服務，以提昇事務所之形象：在會計師業將安全議題加入同步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與安全性增加，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、及組織之安全政策規畫等活動，也更能提供專業化的服務。

由於國內對於資訊安全風險管理的研究甚少，現有劉德泰（2001）將資訊安全風險管理方式，分為四個部分，分別為「風險評估」、「風險辯認」、「風險估計」及「風險策略」等模式；而蔡興樺（2001）則將資訊安全風險管理以 11 個步驟執行，但尚未有針對 Web Services 之安全管理政策加以探討，並提出資訊安全稽核系統整體性架構之研究。因此，更顯示出本計畫之重要性。

三、研究目的

網路服務的核心技術，像 SOAP、WSDL 和 UDDI，可應用於橋接異質的技術領域和傳送文件至企業的作業流程，因此對於會計師事務所而言，可適當運用此一模式建構稽核客戶異質環境的稽核資訊系統。然而為了適用不同客戶類型的應用程式，以及實現以網路服務促進連續性審計稽核模組使用的願景，網路服務的安全技術必須加以重視，以確保網路服務資料的機密和完整性。

因此，本計畫選擇目前 Web Services 相關技術中公認的標準技術 SOAP 為系統平台，在前文中，我們已經說明選擇 Web Services 環境作為我們研究主題的原因，根據我們初步的研究，在現今各類的資訊安全管理規範，並未針對 Web Services 之安全相關議題多加著墨，而運用網路服務，開放式系統下所產生的新型攻擊入侵，也愈來愈嚴重，此乃以 Web Services 為底層通訊機制以建置稽核資訊系統平台的一大缺失。雖然我們過去曾經以 CORBA 作為資訊系統架構之平台，但 CORBA 與 Web Services 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 Web Services 的技術上是沒有的。而 SOAP 乃利用 Uniform Resource Identifier（URI）來代表網路服務的所在參考位置。但因網路服務本質上極易暴露程式和資料儲存的存取，且網路服務間的互動，如企業與供應商間或母子公司間的互動，也可能涉及多個不同安全性技術的參與者，而造成安全系統的不穩定。對冀望以 SOAP 訊息以解決系統溝通問題的企業或會計師而言，HTTP 架構的安全性實在並不足夠。許多更大問題牽涉到沿著路徑傳送訊息的問題，而這種路徑比要求／回應或不涉及 HTTP 傳輸更為複雜。訊息的識別、完整和安全性以及呼叫者，需要透過多重跳躍（Hop）加以保存，因此在傳送路途中可能要使用一個以上的加密金鑰。HTTP 及其安全性機制只解決了點對點的安全性，更複雜的解決方法需要加入端對端的安全機制。由研究動機可知，同步稽核技術是會計師電子商務審計服務的新觀念，目前的文獻多數著重於其對會計專業帶來的利益及輔助電腦查核的方式，至於同步稽核環境下，如何補強現有稽核雛型下的安全缺失與衍生的風險管理問題，則仍付之闕如，欠缺對資訊安全作系統化的探討，因此引發本計劃第一個之研究目的：

1. 探討新的網路攻擊型態，對會計師運用電腦輔助稽核資訊技術所造成的威脅和影響。
2. 研究 Web Services 如何運用其依附於 HTTP 之特性如 Proxy 和 SSL 等，以解決在多點訊息路徑上安全內容的問題，並針對新型的攻擊型態找出防禦的方法，進而達成交易安全之需求。
3. 依據新的網路攻擊方式，在 SOAP 訊息本身內部嵌入安全性或在 Web Application 中設計新的稽核點，以有效偵知受查企業稽核弱點，及時監控受查客戶之交易。
4. 訓練參與研究之工作人員，運用資訊技術以提高稽核效率。

根據前述研究背景與動機可知，隨著資訊運用日益頻繁，除了針對資訊安全的技術面加以控制，亦應由管理面著手。在企業面臨病毒、駭客、惡意破壞資訊的員工等種種資訊安全威脅狀況下，如何確保資訊技術與組織管理兩者得以兼顧，有賴於資訊安全風險管理方法的整合，輔導組織明瞭資訊安全的風險情況，並加以有效處理，以利維護資訊安全，從而讓組織成員明白本身對於資訊安全應有的作為，例如就技術部分，要求資訊系統中所使用的電腦，應具備讓稽核軌跡資料，獨立於運行管理子系統之外，即一般所稱“ 稽核軌跡獨立 ”之功能。簡單地說，此種技術是將電腦系統的運作管理，與安全稽核二大功能完全獨立分開，讓即使是有權力關閉整個電腦系統的管理人員，也無法更改由資訊安全人員所掌管的各項安全稽核資訊記錄，如此便可以確保各項安全稽核資訊不受非法的竄改。

根據過去文獻，大部分偏重於資訊安全的技術方面，對於以資訊安全風險的考量卻

鮮少著墨。但是在實際的資訊社會中，資訊安全的危險卻是存在於我們周遭的環境，而藉由“ 風險管理 ”，以對危險預測並預防，來降低危險的發生，是確保資訊安全的有效方式。因此，本計畫第二個的主要目的有下列幾點：

1.探討 Web Services 稽核環境下之資訊安全需求與風險管理類型。

2.深入研究 COBIT 、ISO17799、BS7799、及 VISA 及其它等國際安全標準政策，並加入 Web Services 環境限制，修正既有的安全政策要項，從而建立網路交易稽核資訊系統之安全稽核政策。

綜上所述，本計畫第二年擬深入研究資訊系統環境下之風險及其內部控制、稽核資訊系統之安全需求、風險及內部控制目標之相關理論等，並配合第一年建構之網路稽核安全架構，讓資訊系統的運作管理與安全稽核兩大功能完全獨立，以加強電子商務稽核系統之風險管理與安全政策。並擬積極檢視各類資訊安全政策、執行管理、教育訓練及技術工程方面之妥善性。

貳、文獻探討

一、網際網路之安全性

1.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。

2.Wright（1999）

Wright（1999）將資訊安全的風險管理分成三個時代，以下說明了不同環境下資訊安全風險管理方式的不同。

表一、資訊安全的風險管理

	環境	威脅種類	風險管理方式	演進原因
第一代	1.固定的資訊設施及環境	1.自然的威脅 2.人員的威脅 3.電腦設施的威脅	1.檢核表 2.基礎資訊安全風險評估	
第二代	1.網路發展 2.環境的分散	1.自然的威脅 2.人員的威脅 3.電腦設施的威脅 4.網路的威脅	1.資產辦認 2.弱點分析 3.威脅分析 4.發生機率	資訊環境改變

			5.衝擊影響 6.安全選擇	
第三代	1.網路應用 2.電腦環境的分散 3.整體資訊系統的建置	全方位的威脅	1.在企業環境下測試及評估資訊安全風險 2.決定何種政策、標準及控制是值得實踐以降低風險及避免疏失 3.提升全體人員對所有可能危害組織資訊安全情勢提升警覺及瞭解 4.評估承諾與控制的效能	需以整體系統全面考量

3.美國財政部金融局（Office of Comptroller of Currency，1999）：

認為可信賴且開放式的網路環境應包括下列幾點：

（1）安全性（Security）：確保任何人未經授權不可進入銀行網路系統。

（2）認證性（Authentication）：客戶銀行及商人能知道交易對象的身分並可如期得到商品及服務。

（3）可信度（Trust）：為了使網路上買賣雙方的交易得以順利進行，需具備公信力的第三者可以確認交易當事人的身份，認證機構即是扮演第三者的角色。

（4）不可否認性（Non-repudiation）：透過電子證書的設計，使發出交易信息的人無法否認曾經發送此筆訊息。

（5）隱私性（Privacy）：防止消費者個人資料被不當使用。

（6）可用性（Availability）：確保網路系統的更利通暢。

4.Sofia Giannakoudi（1999）：

認為網路銀行安全機制應包括二個層面：

（1）訊息安全性（Security of the message）：係指客戶與銀行交易的主要特性，必需是確認性（authenticity）－使用者身份的識別（identification）；完整性（integrity）－傳送的資料無法更改；不可否認性（non-repudiation）－防止交易完成後否認；隱密性（Confidentiality）－保護資訊被竊聽。

（2）安全的環境（Security of the environment）：已存在的銀行資料與客戶的資訊，應建立完成內部控制的指標與其他安全防護措施。

二、會計師事務所之安全性服務

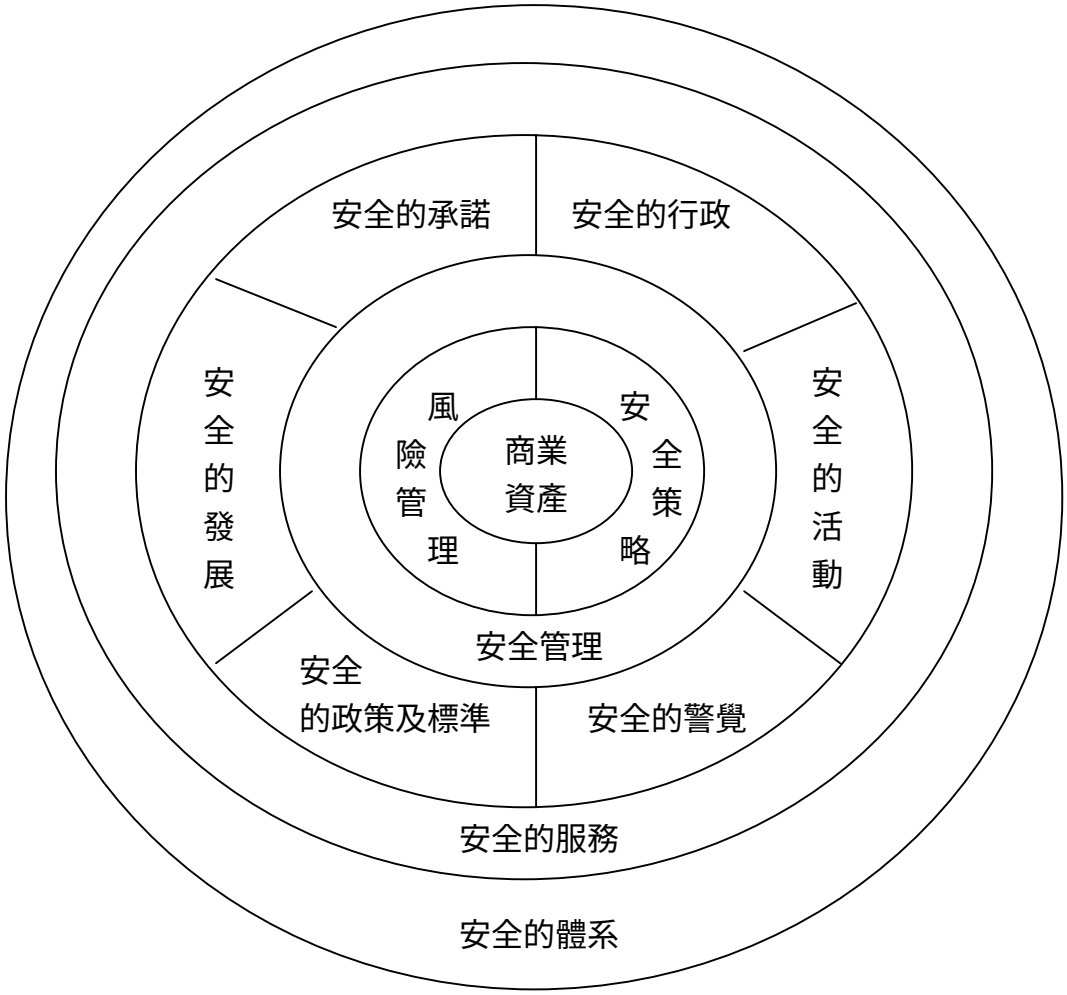
1.Pricewaterhouse Coopers (PwC)[1]

PwC 的安全服務乃一全球性的風險管理業務（GRMS），其業務範圍包括公司的風險管理服務、週期性的安全評估、設計、執行以及經營。在 GRMS 下 PwC 廣泛地檢視企業的安全政策與風險，除了基礎建設外，並在商業過程中的安全／控制以及資料的健全完善上提供以下的建議：

- **安全的威脅及缺失弱點的評估服務。**PwC 的安全的威脅及缺失弱點的評估服務著重在確認委託人的安全風險及安全基礎建設。利用分析結果提供安全技術及管理的建議以降低風險。
- **事業的安全結構服務。**PwC 利用內部的研發架構以及網路基礎應用，如：事業的安全結構系統（ESAS），來設計及實施有效的資訊安全架構。運用 ESAS 功能的應用安全及管理知識以及重視 ERP（SAP，Peoplesoft，and Oracle）各提供管理鍊。
- **安全整合服務。**PwC 的安全整合服務包含商業個案的發展、設計、構建及執行。公司也整合這些技術到許多常見的商業應用平台。
- **管理安全的解決（MSS）。**MSS 服務提供委託人安全的監督，並已建立之加值安全的服務內容有品質控制，電信安全事件以及場地提供。
- **防電腦犯罪的服務。**PwC 提供兩種類型的防電腦犯罪的服務：緊急反應及電腦預測訴訟結果。公司已經發展一個關於網路的調查小組，可使稽查人員從以前的合法部門成員的電腦犯罪以及智慧財產部分，瞭解影響網路如何侵入，如何能欺騙系統運作等。
- **e-Trusted 的服務。**進行網上信任之認證服務，PwC 提供安全的線上確認及進行數位認證執等多項功能。

2.Accenture[1]

該公司提供一系列資訊安全諮詢及系統整合的服務以及互補的服務。透過啟動器、起點、或是完整的檢查。此安全架構的內容如下：



圖二、Accenture 的安全架構

三、稽核資訊系統使用之主要科技

1.網路服務（Web Services）技術

網路服務結合了應用程式的程式執行特性和網際網路的抽象概念，能讓任何的作業系統、硬體和軟體相容。以網路服務為基礎的網際網路基礎建設，採用這個抽象層級概念，包含和資料相關的語意資訊。也就是說，網路服務不僅是定義資料，也定義如何處理資料以及在資料和底層軟體程式之間作轉換。

網路服務需要數個以 XML 為基礎的相關技術，傳輸資料並在資料與程式、資料庫之間作轉換。茲說明如下：

- **XML（可延伸標記語言）**，是網路服務建構的基礎，提供一種語言來定義何謂資料以及如何處理資料。XML 代表一組相關的規格，這些規格是由全球資訊網聯盟（W3C）和其它組織所公佈及維護。
- **WSDL（網路服務描述語言）**，是一項以 XML 為基礎的技術，定義網路服務介面、資料和訊息型態、互動模式和轉換協定。
- **SOAP（簡單物件存取協定）**，是一組以 XML 為基礎的技術，定義網路服務通訊

的信封（envelope），能夠對應到 HTTP 或是其它傳輸協定，並且提供 XML 文件在網路上的傳輸，一個連續化的格式，和 RPC 互動的協定。

- **UDDI（通用描述尋找和整合），**是一個網路服務註冊和尋找的機制，用來儲存和分類企業的資訊，以及取出指向網路服務介面的指標（pointer）。

2.SOAP 規格〔14〕

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。

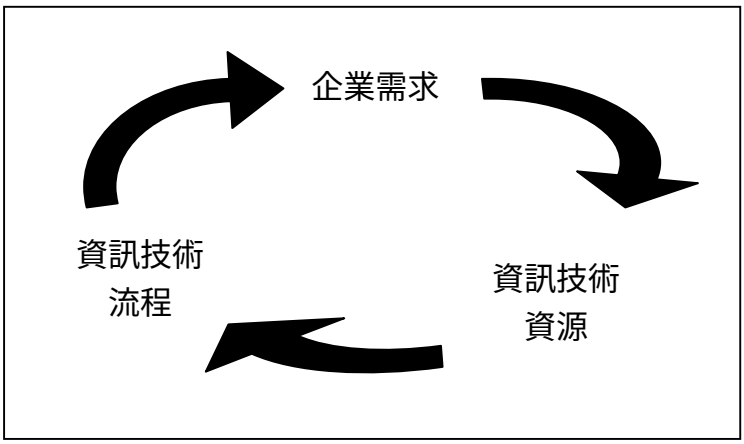
四 相關資訊安全管理架構及標準

1.COBIT[9、16]

資訊系統稽核與控管協會（Information Systems Audit and Control Association, ISACA）於 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。〔9〕

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，此三要素間之交互關性如圖四，COBIT 架構可提供管理當局、使用者、稽核人員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。



圖三、COBIT 內部控制三要表

2.英國國家資訊安全管理標準－BS7799[7、8]

BS7799 是英國國家標準協會(British Standards Institution, BSI, 1999)所制定之資訊安全標準，BS7799 第一部份已在 2000 年 12 月 1 日成為 ISO/ICE17799 國際標準(樊國楨，1999)。資訊安全管理目前在國內尚處於啟蒙階段，已由行政院國家資訊通信基本建設計畫專案推動小組及經濟部標準檢驗局聯合指導。此套資訊安全管理標準，除於英國使用外，已有荷蘭、丹麥、挪威、瑞典、芬蘭、澳洲、紐西蘭、南非等國採用，日本、瑞士、盧森堡等國亦對 BS7799 深表興趣。

3.VISA[27]

在 B2C 的網路商務中，Visa [Visa00] Visa 的安全標準較為大眾化，可以運用在許多的商業上面，對 B2C 和 B2B 來說也非常的合適，尤其是線上即時交易的商業模式更需要此系統。VISA 的安全標準涉及的安全範圍自『商業控制』到『網際網路安全控制』和『人事政策和訓練』到『網頁安全控制』等層面。雖然 Visa 的安全指導方針有包括到人事管理層面和交易行為層面，但是缺少對客戶和合作經銷商的安全教育項目，所以 Visa 還要加強在安全教育的措施，以達成全面安全措施。[https://wow.mfi.com/csi/order/publications.html]。

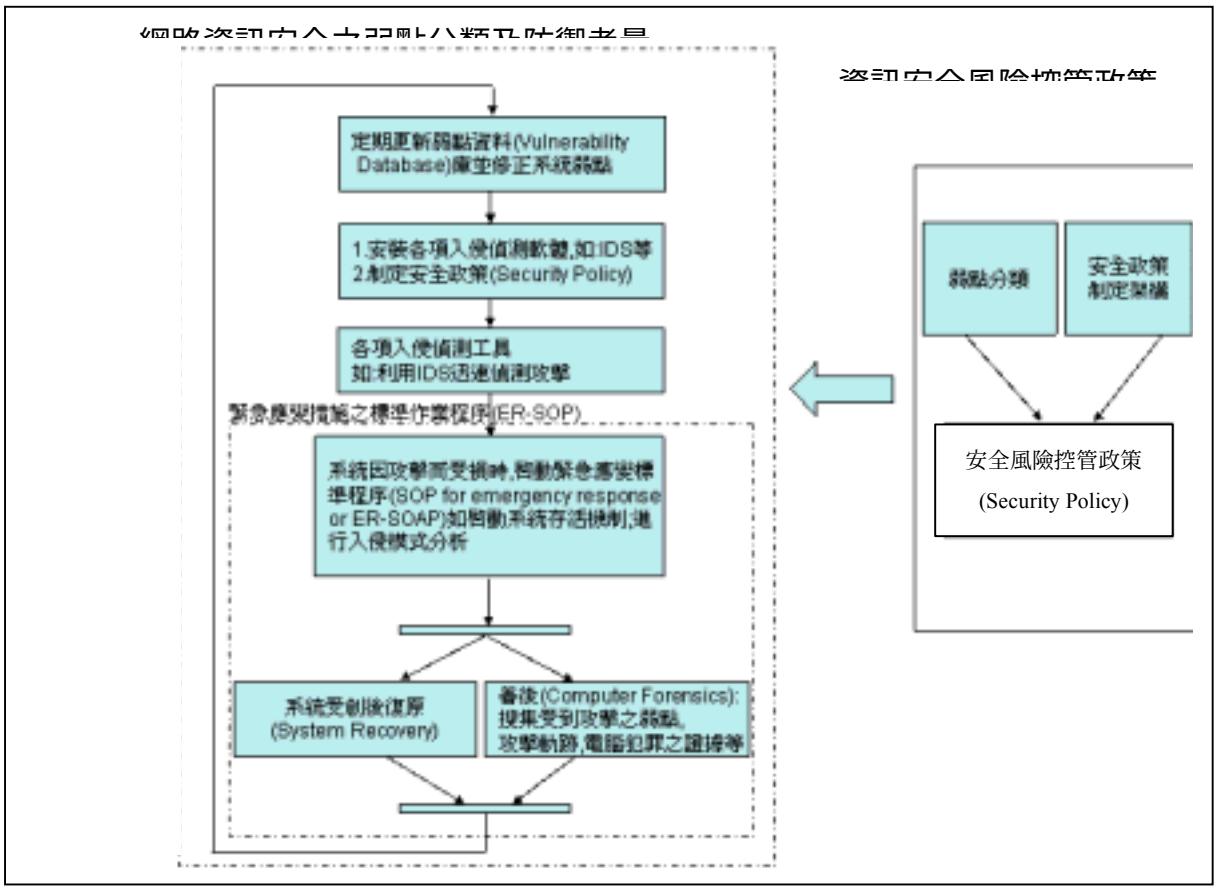
參、研究方法及進行步驟：

我們在民國 91 年度便已執行一個一年期的國科會計畫，開發一個適用於 B2B 電子商務系統下，且能夠跨越不同 EDP 系統平台，以 SOAP 規格為基底之稽核資訊系統雛

型，以達成同步稽技術之目的。今年本計畫延續過去研究的基礎，進一步提出一個基於現有技術下的稽核資訊安全架構，及探討在網路服務環境下之風險管理政策，冀望兩者相輔相成，以實現整體稽核的安全性。本計畫將分成二個部分，第一部分，首先整理網路服務(XML、WSDL、SOAP 及 UDDI)之相關文獻與資訊安全技術，檢討新型的網路攻擊型態對網路服務安全之威脅，設計一套安全可靠的 SOAP 平台，利用此架構建置具有高度開放性的異常反應系統，以強化稽核資訊系統的安全性；由於網路服務可以方便會計師跨越不同受查客戶的 EDP 平台，來做資料的存取與轉換，因此本計畫也擬在 SOAP 平台上，嵌入適當的控制點或監控機制，從而提高稽核系統之安全架構與服務的內容。除了由技術面來加強 Web 環境下之安全性外，第二部分則預計由管理面探討受查企業資訊系統的風險管理與控制，從而建立有效的企業網路服務安全政策。並擬採用 COBIT、BS7799、 ISO 17799、VISA 等資訊安全管理標準，加入對網路服務開放系統下各類新型入侵攻擊與人為因素之安全考量，以提出適用於電子商務之企業資訊安全管理政策。另外，根據文獻探討與專家訪談之結論，將會計師界之稽核資訊系統與受查客戶之安全作業系統相整合，以驗證稽核資訊系統模式中所設立之安全機制與內部控制是否符合所需。茲將此二部分，分述如下：

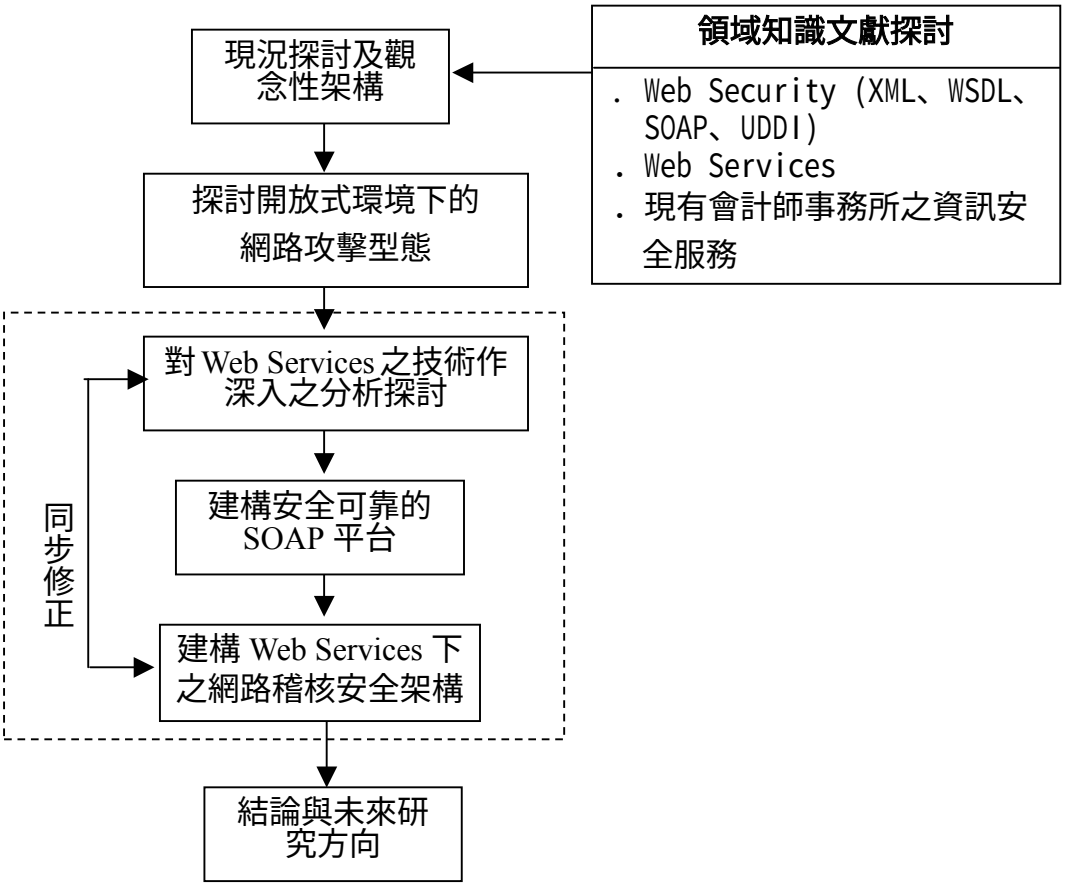
第一部份之工作計畫：

e 世代的審計專業服務的拓展如連續審計、跨平台的電腦輔助稽核業務等，都在在要求會計師專業能提供及時可靠的財務資訊。資訊安全層面的考量除了上述之技術問題外，許多存在於現實狀況中的安全漏洞，其實是源自管理層面需求不明確所造成，安全的網路技術必須配合良好的安全政策才能發揮其應有的效益，而維護網路安全(Web security)最有效的方式，應先在組織內部依據弱點分類，評估組織內的安全風險與管控政策以發展出 Web Services 系統下之資訊安全探管政策，希望藉由對資訊系統的稽核管理，以期提昇整體的資訊安全。



圖四、 網路資訊安全之弱點分類及防禦考量

一、研究流程：



圖五、研究流程（第一年）

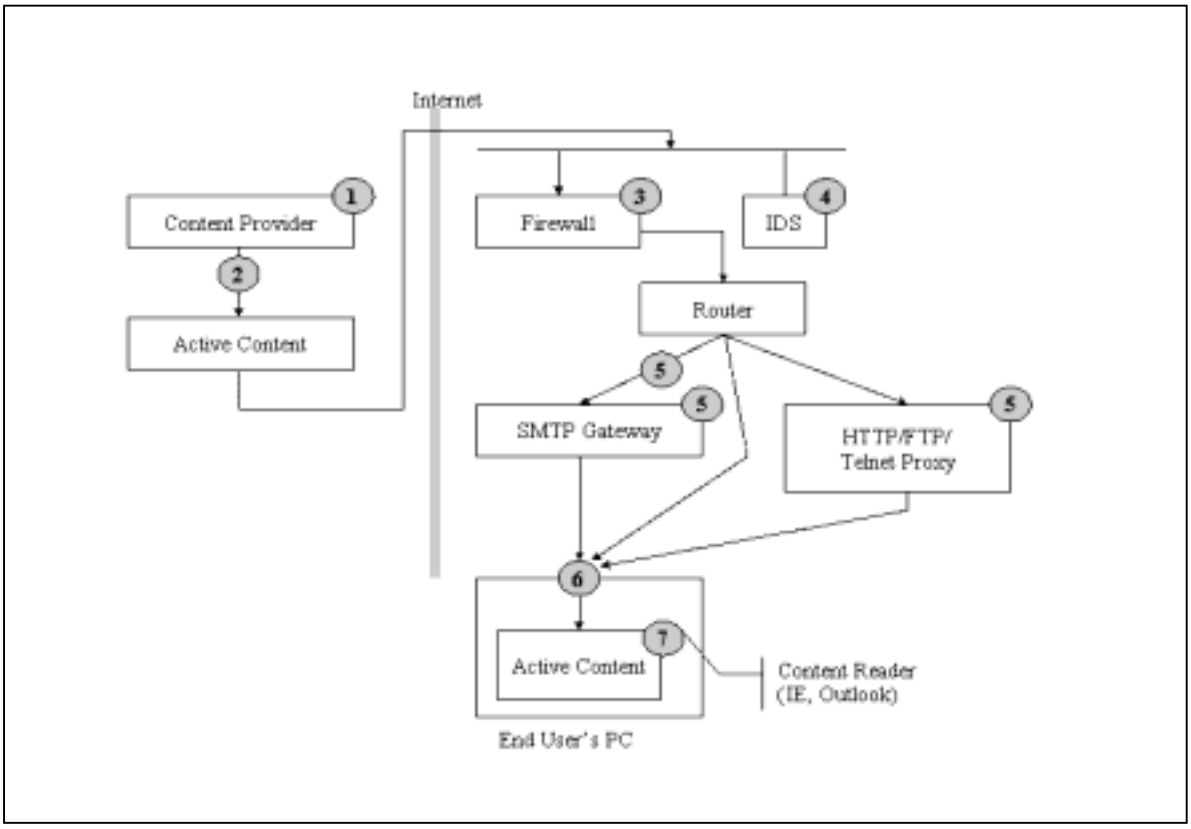
二、研究步驟：

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。本計畫藉由對上述環境之了解以建立同步稽核系統下之網路稽核安全架構，另外在技術方面彙整網路服務(含 XML、WSDL、SOAP、UDDI)與電腦審計技術之最新發展及研究，其次參考本人 91 年度國科會計畫之同步稽核資訊系統架構，以了解其對審計資訊系統之安全性需求。

（一）探討新的網路攻擊型態對網路服務稽核的影響：

新攻擊程式最常被放在網頁上或經過 e-mail 被傳送給使用者。由於瀏覽器當初 Microsoft 與 Netscape 競爭激烈，兩家公司都企圖在短期內把一個簡單的 HTML 解讀器升級為一個完整的軟體平台（application platform）。為了達成這個目的，兩家公司將網

頁和 e-mail 的內容得以從靜態（static）提升為動態內容（active content）。這種動態內容不但可以帶給使用者視覺以及聽覺上的享受，更可以支援 e-commerce 所需的各種複雜的互動模式。但也由於軟體發展過快與功能過度複雜，造成軟體漏洞百出，因而提供了攻擊程式一個完美的入侵窗口。使用者目前只要瀏覽某個網頁或收到某封 e-mail，網頁或 e-mail 中的入侵碼，則可輕易地利用瀏覽器的軟體漏洞進行入侵。過去研究所提出之同步稽核架構或連續性審計，雖然能為會計師與受查企業帶來諸多效益，然而，在開放式的網路系統上，受查企業之機密資料極易直接暴露於公眾網路上，因此本研究擬先探討新型的網路攻擊型態，對會計師網路稽核業務推展與資訊安全之影響。茲將目前安全技術的防禦措施，列示如圖六。



圖六、安全技術的防禦措施

上圖的七點防禦措施分別為：1.防毒軟體(AV)，2.程式簽章(Code Signing)，3.網路防火牆(Network Firewall)，4.入侵偵測系統(Intrusion Detection System)，5.內容過濾器(Content Filters)，6.個人防火牆(Personal Firewalls)，7.安全沙盒(Security Sandbox)等。

（二）選擇一個安全可靠的 SOAP 平台：

為使連續性審計系統達到在異質環境順利運作的目的，本研究採用 Java 語言撰寫 SOAP 介面以作為雛型系統開發之核心介紹如后。

Java 語言是昇陽公司(Sun Microsystems, Inc.)在 1990 年初所設計的一種程式語言。最初 Java 小組的原意，是設計一種能被廣泛應用於消費電子用品(consumer electronic devices)的程式語言，但因種種原因，JAVA 並沒有達到原先所預期的商業目標。由於全球資訊網 (World Wide Web) 及網際網路(Internet)的蓬勃發展，卻促使 Java 語言重新為業界廣泛使用，原因是 JAVA 具備物件導向的(Object-Oriented)特色所致：(1)簡單(Simple)，(2)安全(Secure)，(3)解譯(Interpreted)，(4)可攜性(portable)，(5)中性架構(Architecture-neutral)，(6)多線式(Multithreaded)。

相對於其他種類物件導向(Object-Oriented Programming, OOP)語言，Java 較容易學習。因 Java 的語法類似於 C 語言，較容易被設計師接受；再加上 Java 原始設計即為能應用於各種消費電子產品，因此 Java 語言具有可攜性的特性，也就是說，Java 程式可執行於不同的處理器或硬體；也由於中立性架構的(Architecture-neutral)特性，因此 JAVA 可在不同平台上執行 (platform-independent)，其運作方式參見附錄一，JAVA 之封包佈局如附錄二。

SOAP（Simple Object Access Protocol）於 1999 年由微軟與 Lotus、IBM 等大廠提出。SOAP 使用較為簡易的方式，表達分散式環境中資訊交換的協定，主要是使用良好格式（well-form）的 XML 語言，做為封包外型語言，並結合 HTTP 與其衍生架構，形成資料傳輸通訊協定架構，使得資訊交換更為順暢。SOAP 所扮演的角色就是提供一個機制用來決定哪一個物件被 SOAP 所呼叫，也就是使用一個現有的連續通訊協定，在一個普通的傳輸層上，連續呼叫遠端程式中的方法。W3C 已將 2000 年 4 月下旬所提出的 SOAP1.1 版納入其註解中。

在 SOAP 的 1.0 版中已指出其設計目標為：

一. 使用 HTTP 為傳輸基礎並運用 XML 做為編碼方式，在 Internet 的標準上提供一種標準的物件呼叫通訊協定。

二. 建立一個具有延伸能力及未來發展的通訊協定及封包負載格式（Payload format）。

SOAP 除了在 1.1 版明確指出「簡單性與延伸能力」的特點之外還具有下列優點：[1]

一、 建立在開放的技術之上：不需另外授權，所有使用者都可以自由取用，因此普及率更高。

二、 成為單一規格：可以結合各種通訊協定，增強資料的互通性。

三、 支援 HTTP 第 80 埠：由於許多防火牆僅開放 HTTP 第 80 埠供資料存取，因此可以讓資料交換沒有障礙。

四、 支援其他程式：SOAP 可以支援其他較不嚴謹的分散式應用程式。

五、 不影響應用程式使用通訊協定：由於 SOAP 具有強大彈性，因此也不影響影應用程式的運作。

六、 跨平台的資料傳輸協定：SOAP 封包內的資訊都是純文字且遵守著 XML 的規範，純文字的內容可以被很多系統所接受，因為現今大部分的電腦都已經

[1] http://static.userland.com/xmlRpcCom/soap/SOAPv11.htm

把純文字當成輸入的方式。

簡而言之，SOAP 是一個可以隨心所欲（lightweight）建立在 HTTP 上，並以 XML 為描述編碼的連續畫參數資料交換環境，可應用在作為分散式物件溝通的簡單協定。

運用 SOAP 的動機如下：

一、目前已有許多的分散式物件架構(CORBA, Java RMI, DCOM…)存在，但彼此間並無一個標準的協定，作為這些異質分散式物件彼此交換資訊用。SOAP 即扮演著溝通異質分散式物件橋樑的角色。SOAP 結合了已為業界所接受的 HTTP 作為底層的通訊協定，以越來越普及的 XML 來描述資料，以期能為業界所接受，成為標準。

二、由於企業廣泛使用防火牆保護內部網路, 僅開放少數 port(如：http port 80), 使得很多分散式物件無法穿透防火牆, 對發展者來說是件頭痛的事， 而 SOAP 走的是 HTTP (port 80), 可以在大多數的防火牆遊走，SOAP 與其他分散式物件技術的比較如表三。

表二 SOAP 與其他分散式物件技術的比較

	SOAP	CORBA	DCOM	JAVA RMI
延展能力	由於使用 HTTP 因此就有良好延展性。	有狀態的程式設計模型，必須透過 PAM 才能達成，延展能力欠佳。	以確保在遠端程式呼叫中所有關係的事物都可以保持運作，不太考慮延展性的問題，無法負荷超量用戶的情形，延展能力欠佳。	由於使用 HTTP 因此具有良好延展性。
效能	必須同時考慮 XML 的轉譯，可能會造成效能的降低。	獲得物件參照之後，允許伺服器和用戶端直接互動。	需要數個循環呼叫才能啟動，運用 OBJREF 方式可以直接存取，但循環呼叫的次數也會增加。	可以在 JAVA 的架構做出有效能的協定。
啟動	將啟動交由執行 SOAP 的通訊協定來執行。	發出訊息給 ORB 後還需特定物件的轉接器，程式的啟動需要數個網路循環才能達成。	運用 SCM 技術，需要兩個步驟，也可以透過 proxy 進行啟動，啟動狀態良好。	當 RMI 啟動遠端物件，需執行 JAVA 類別的物件，就會傳送到用戶端。
狀態管理	由於使用 HTTP 做為傳輸方式，因此是屬於無狀	需實行 IIOP 及 GIOP，以 Connection -oriented 型式維	用戶端可以自由管理需要的狀態資訊，但是不能在沒有特	用兩個 Connection -oriented 型式維護方程式之

	態的協定，由 HTTP 規範要求與回應的架構。	護方程式之間的的狀態資料，管理良好。	定介面下使用。	間的的狀態資料，管理良好。
資源回收	不會去管理，需由使用 SOAP 的分散式物件協定管理。	由於 GIOP 及 IIOP 並不支援, 因此 CORBA 並沒有分散式管理。	假如連線中斷，物件系統會等待兩個額外時間(六分鐘)，之後回收伺服器資源。	由於運用 JAVA 的原生架構，因此就像 CORBA 及 DCOM 實行分散式物件的參照技術來維護遠端的實體。
安全性	並不執行任何安全機制，但因為是以 HTTP 為傳輸方式，因此借用 HTTP 的安全規範。	使用 SSL 在 TCP/IP 上達成。	可以用純文字或加密方式傳遞，強調驗證、授權及辨認。安全性優良。	運用 JAVA 及 RMI 本身的安全管理。

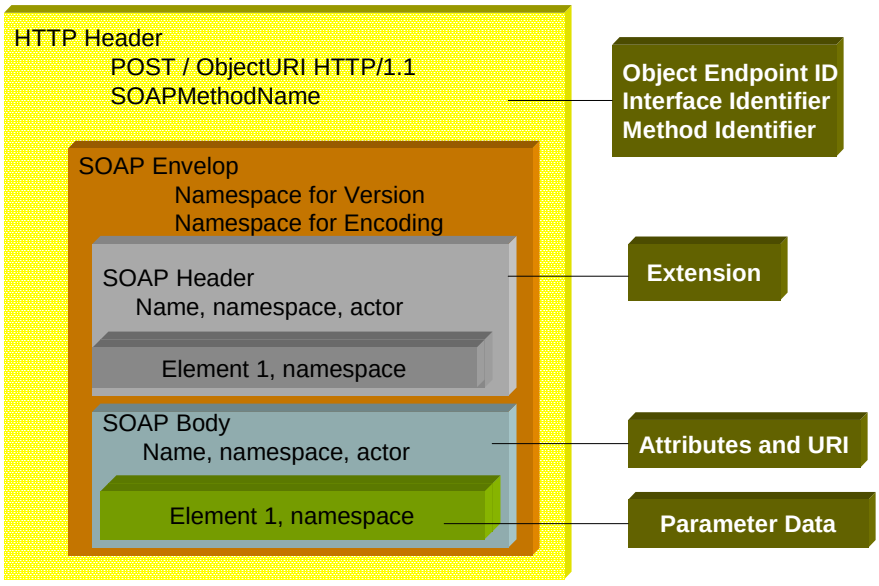
資料來源：紀東昀 “連續性審計需求及雛型架構之研究”，2003

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 的 Message Structure 如圖八所示。主要區分為三個部分：

1.SOAP Envelop.

2.SOAP Encoding Rule.

3.SOAP RPC Representation.



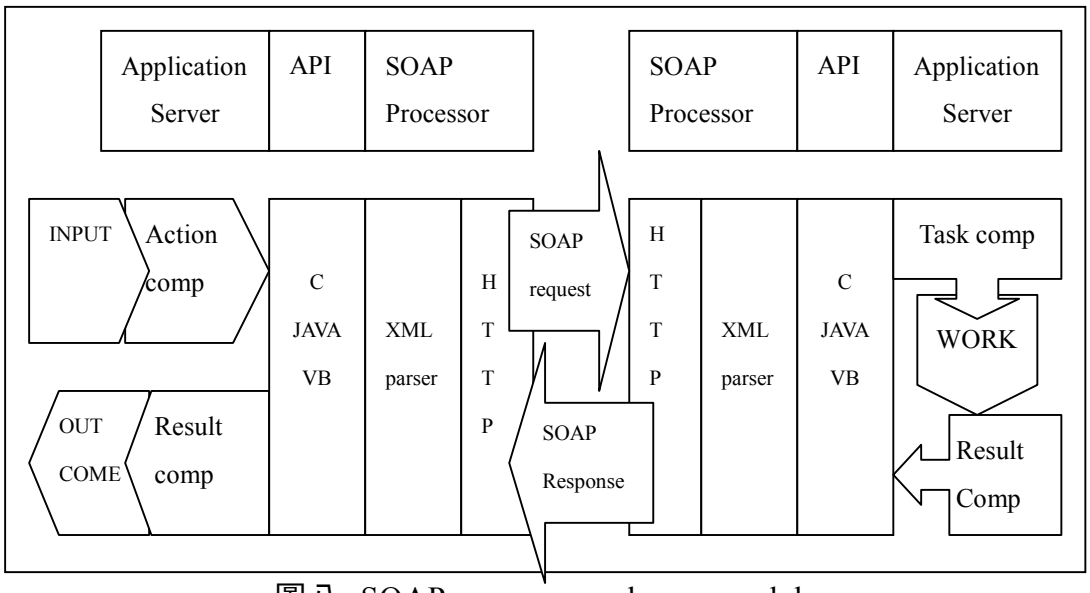
圖七、Message Structure of SOAP

（五）建構 Web Services 下對應之稽核介面與資訊安全架構

本計畫參考國內外稽核資訊系統作業相關的研究報告及期刊，以及過去 2 年執行國科會稽核資訊系統架構的經驗，由於 SOAP 標準被認定是未來 Web Services 之主要標準，而目前 SOAP 1.2 又尚未考慮安全(security)以及可靠性(reliable)等相關議題，因之，本計畫主要的目的在於建構一個安全可靠的 SOAP 平台(reliable and secured SOAP platform or RS-SOAP)，並利用此架構建置(install)一套具有高度開放性的異常反應系統(incident response system, or IRS)用以處理稽核資訊系統不可避免的各式異常事件，包括入侵、攻擊或是舞弊等事件。經由我們實做研究雛形(prototype)的經驗來驗證此標準界面之可行性(concept-proving)，作為日後稽核資訊系統評估時之安全考量因素及系統整合廠商評選之要點

在建構具安全性的 SOAP 平台後，本計畫將初步設計執行同步稽核所需用的網路服務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。由於作業流程對自動化企業內部、或 Web 上企業作業之間的互動，是很重要的。因為作業流程定義了一連串的互動，像是完成一筆購買訂單、處理旅遊的訂位、或是執行生產計劃，所以作業流程通常也稱作「編排」。在充分瞭解作業流程後，即可在開發的 SOAP 平台上設計監控模組（Continuous Monitoring Module），以監督跨企業之電子商務的作業，遇有異常狀況，則產生例外報告給稽核人員。此交易安全監控模組主要的應用如下：(1)駭客入侵風險的監督。（2）高風險交易的監督。（3）偵測詐欺。（4）產生例外報告。（5）監督網路服務的安全性，如機密檔案的存取與密碼的使用等。

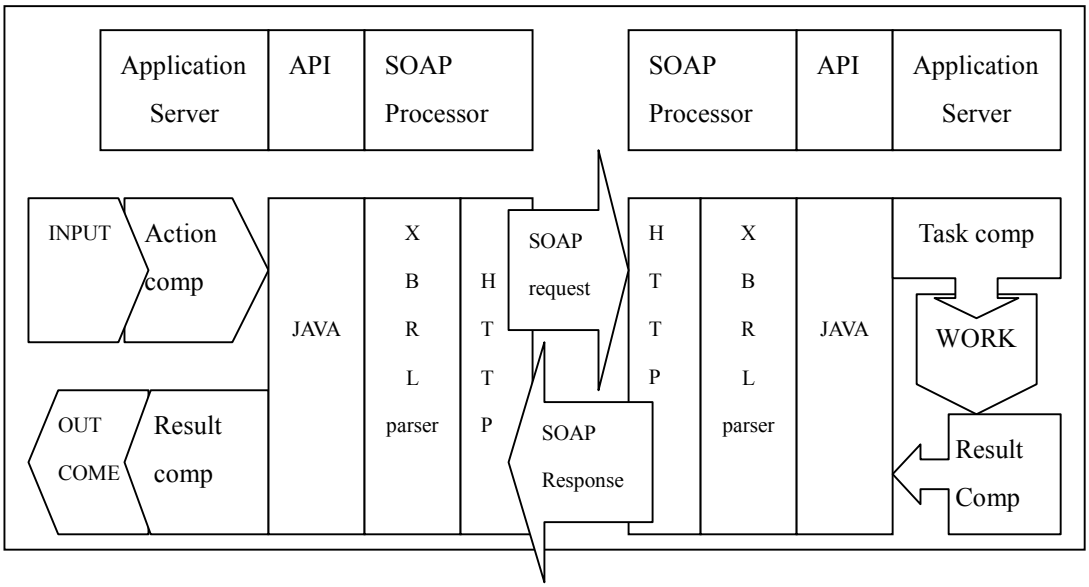
SOAP 較其他的分散式架構，更是適用於異質環境的整合上，若以 SOAP 為分散式的架構，其訊息交換模式如圖九：



圖八 SOAP message exchange models

資料來源： Kenn Scribner, Mark Stiver, Kennard Scribner, (2001).

由此可知， SOAP 是將 XML 做為描述的語言，當 SOAP 做為商業用途時相較於其他分散式物件技術，更容易將 XBRL 整合於 SOAP 之中，對於通信協定的本身不需做重大修改，不論是在複雜交易環境下的民間企業或是擁有眾多子系統的公務機關都非常適用。因此將 XML 替換為 XBRL 且運用 JAVA 撰寫 SOAP 介面之後的訊息傳遞方式如圖十。



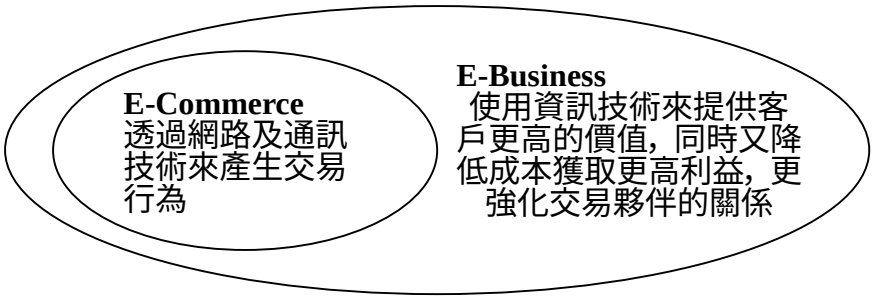
圖九、運用 XBRL 及 JAVA 之後的 SOAP message exchange models

第二部分之工作計畫：

二十世紀最重要的一項革新無疑是「資訊技術革命」，它顛覆了人類既有的世界觀，將人類帶入一個無國界的新紀元。現代企業的辦公室可說是資訊時代下的產物，稱之為電子化企業。總括各學者、專家對於電子化企業及電子商務的各項定義如下：Jarvenpaa 及 Tiller（1999）認為當企業利用電腦網路及電子郵件或企業內部系統去支援企業間的線上商業活動交易時，即定義為「電子化企業」；Smith（2000）認為利用數位技術來達到企業營運最佳化者，即為電子化企業；林佳璇（2001）電子化企業是指以網際網路為基礎，在資訊技術架構下，進行管理流程的數位化以及成員思考與決策模式的 e 化，結合虛擬與實體環境的企業經營模式。

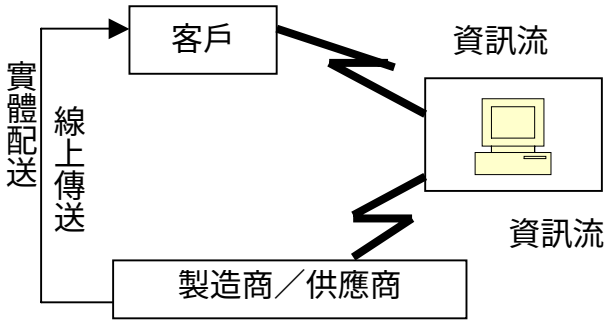
Kalakota ＆ Whinston（1996）認為電子商務係「利用電腦網路與資訊高速公路來銷售與購買資訊、產品、服務等行為，其目的在因應公司組織與商人需求，達到降低成本、增進商品與服務的品質、加強服務提供效率的目標。」吳琮璠（2000）認為是泛指「利用資訊網路進行商業活動，包含商品交易、廣告、服務、資訊提供、金融匯兌、市場情報與育樂節目販售等」；黃景彰（2001）認為「電子商務」，指的是「電子化的商業形式，透過網際網路作為訊息溝通的管道。」

電子商務係電子化企業範圍下的一環，由圖十中可明顯看出兩者的關係：



圖十一　EB 與 EC 的關係圖　資料來源：洪基華，民 90

電子商務的交易模式如圖十二，客戶透過網路以資訊流的方式下訂單給製造商或供應商，製造商在接受此訊息後回傳資訊給客戶，並透過務流的方式將產品送交至客戶手中。利用電子商務的方式，可使企業節省大部分的時間及交易成本，並可擴大其銷售通路，使企業獲得更多的利潤。



圖十二　電子商務下之交易方式

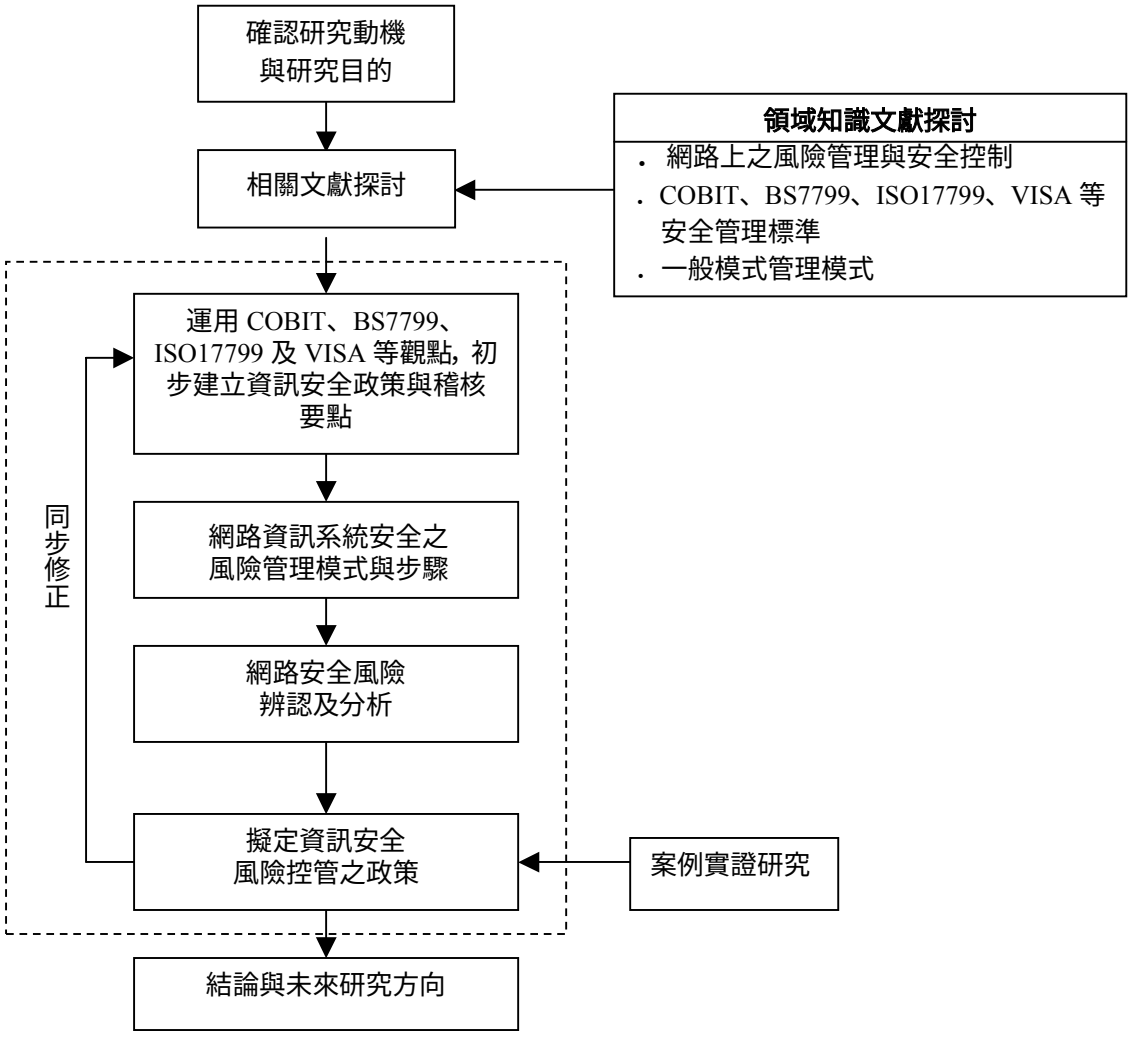
企業之所以要不斷的投注資源於電子化工程上，不外乎期望以科技來改造企業的營運，並取得及保持競爭優勢，促使經營績效更進一步改善，以確保企業持續的成長與獲利。在夏安齡（2000）的研究中表示企業在導入電子商務過程中會受其內部控制有效程度影響。企業在導入電子商務時，若沒有一個有效的內部控制，則無法達到電子商務的成效。歐文純（2001）也表示在科技快速發展的今日，沒有人能保證百分百的安全；尤其是當安全的環境產生漏洞後，需要內部控制與內部稽核機制的輔助作為最後的防線來偵測環境的漏洞，以減少公司的損失。因時代的變遷，傳統企業運用電子商務的營運模式也逐漸增加，企業組織對電腦資訊系統的依賴度相對提高，但對企業而言，若想要跟上電子化時代的腳步，一套有效的管理機制，才是獲取競爭優勢的關鍵。

由於網際網路的快達發展，目前其所使用的通訊協定（Protocol）TCP/IP 已成為各個網路彼此交換訊息的標準。會計師與受查企業間可以利用簡單的郵件彼此通訊、利用檔案傳輸協定（File Transfer Protocol：FTP）來上傳或下載檔案資料、亦可以利用超文件傳輸協定（Hypertext Transmission Protocol：HTTP），藉由適當的瀏覽器（Browser）軟體，來擷取網路上各個 Web 伺服器所提供的網頁（Page）訊息。過去我們以分散式系統開發會計師事務所的稽核資訊系統[21、22]，須透過特殊的通訊協定，如 CORBA 或

是得在特定的平台上依照特定的語搭配使用。但隨著 Web Services 的發展，已進展到以 XML 作為訊息傳遞的基礎，在 SOAP（簡單物件存取協定），WSDL（描述語言），UDDI 等技術，在不同平台上執行物件，這種新的觀念將改變原有系統整合的方式，進而解決分散式架構間的溝通問題。

雖然網路服務（Web Services），替以往困難的系統整合問題找到了解決方案，但許多實際上的應用以及標準，目前還停留在探索階段。以網路服務機制設計的連續性審計技術與同步稽核架構[7、8、17、33]雖然能為會計師與受查企業帶來諸多效益。然而，在開放式的網路系統上，受查企業之機密資料極易直接暴露於公眾網路上，且 SOAP 的安全機制僅限於點對點的安全性，更複雜的解決方式須透過端對端的安全性（Scott Seely, 2002），另外對於來自網路上的威脅，與會計師與企業間作業流程的互動是否可以開發網路服務平台上之監控模組，以監督跨企業之電子交易或入侵。因此激發了本研究探討網路服務中之安全與風險，並將之應用於同步稽核資訊系統架構之動機。

一、研究流程：



圖十二、研究流程

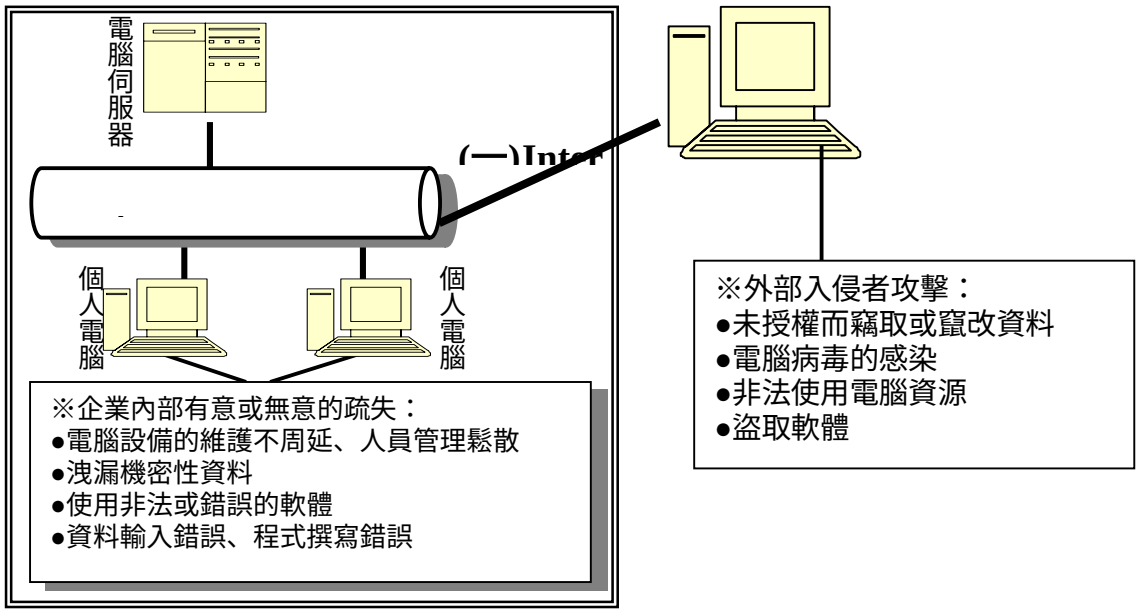
二、研究步驟：

（一） 資訊安全及威脅來源

從 1990 年代開始，由於全球資訊網（World Wide Web）的發展，再加上資訊技術的不斷提昇，使得網路幾乎成為現代人的倚賴對象。有了網路的幫助，企業也致力於將傳統的人工作業轉換成電腦連線作業，不但降低交易成本、省時省力、更強化企業的競爭力，因此網路可說是企業的必要配備之一。然而提到網路的優點，就必須強調它的缺點：(1) 企業內部的資訊安全控管一旦產生漏洞，職員藉由職務之便盜取或修改資料，將造成企業莫大的損失；(2) 網路的無遠弗屆，使得外界有心人士可藉著網路從事各種攻擊行為，例如病毒散播、資料竄改及竊取等等，對企業造成的損失也將難以估計。如此的內憂外患夾擊之下，資訊的安全與控制成為目前首當之務。

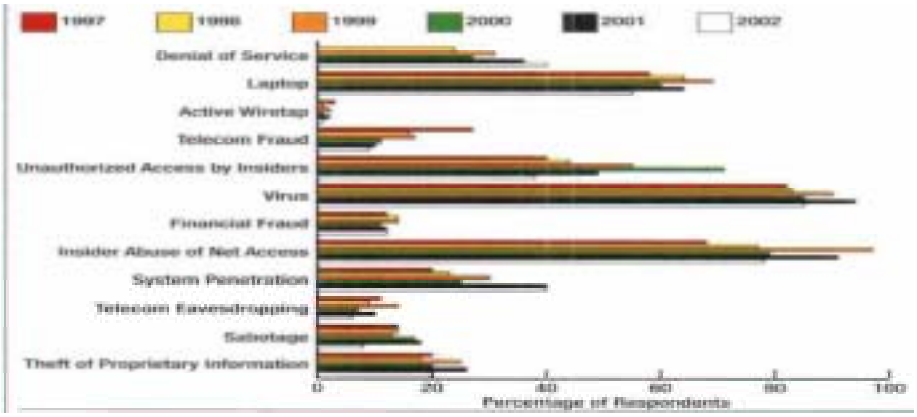
所謂的資訊安全主要是指與電腦相關的資源，例如：電腦軟硬體配備、周邊配備以及網路安全等。各學者、專家對於資訊安全的各項定義如下：Dam and Wesley（1997）認為電腦的安全性旨在探討電腦環境軟硬體元件的損害，而目的在於資訊的保密性（confidentiality）、完整性（integrity）、可取得性（availability）、合法性（validity）；吳琮璠、謝清佳（2000）認為電腦的安全管理主要在保護電腦資源，包括硬體、軟體、資料、人員，以防止變更、破壞電腦資源及未授權地使用電腦資源；Kees（2002）認為軟體的應用安全指的是只有透過認證程序及系統認證的合法人員才可以使用，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。而綜合上述專家、學者所分類的各項資訊安全的破壞來源，可將其分成企業內與企業外兩種，如圖十三所示：



圖十三　資訊安全的破壞來源

由於現代辦公室每日的工作，大量依賴電腦的輔助做資料檔案的傳輸及存取，加上網際網路的發展，使得電腦系統的範圍更加擴大，若有一個環節發生錯誤，有心人士便可輕易的透過網路竊取資料或破壞系統，很容易使一切的作業發生混亂。



圖十四　網路攻擊及濫用的統計　　資料來源：美國電腦安全協會，2002

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發現，資訊安全的威脅來源大多數係來自公司的內部。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。

（二）相關的資訊安全內部控制標準

全球性的競爭環境已經來臨，企業組織的作業方式也持續在改變，在強調競爭優勢及成本效率的環境中，自動化企業是不可改變的事實。一個好的企業組織必須對 IT 的風險和限制有正確的評價及基本的瞭解，以達到有效率的領導及適當的控制。為了維護資訊安全，世界各國政府、企業、民間組織無不致力於制定相關的資訊安全控制標準，以下就一、SAS 94；二、SP800-14；三、SP800-27；四、ISO 15408；五、ISO 17799；六、COBIT 相關的資訊安全內部控制標準加以比較（表三）：

表三　相關資訊安全內部控制標準之比較

	SAS 94：進行查核時資訊技術對內部控制考慮事項的影響	SP800-14+27：用於保護資訊技術系統的一般公認原則與執行	ISO 15408：用於資訊安全的評估標準	ISO 17799：資訊安全管理的標準	COBIT：資訊與相關技術的控制目標
應用安全的方法	著重在處理財務交易及會計分類帳的應用安全。	在每個生命週期階段的執行及控制;操作上的控制。	防止未經許可的揭露、修改或遺失;用於開發者的指導方針及使用者的確	防止損失、用戶資料的修正或誤用、輸入、處理、產出控制、加密和應用發	有關 IT 程序的規劃、取得、發展、支援及監督運用的安全與控制。

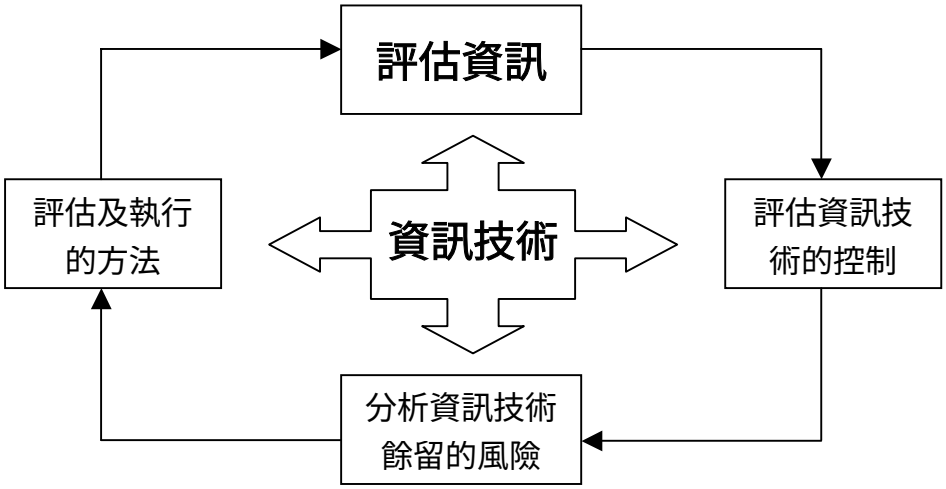
			信。	展的控制。	
目標	整合所有影響財務及審計報告的資訊。	用於管理資訊及資料系統的使用、防護及設計的安全原則及應用。	訂定有關衡量 IT 的安全及確信的標準。	設置一套最好的資訊安全執行控制。	在企業需求、IT 程序及 IT 架構裡的安全管理。
重要因素	控制環境、風險評估、控制活動、資訊與溝通、監督	8 個應用原則及 14 項實務準則(SP800-14)；生命週期階段的 33 個安全原則(SP800-27)	安全的"功能"和"確信"的要求用來評估 IT；評估確信的水準	涵蓋資訊技術安全所有方面的十個領域。	範圍： 規劃及組織、取得及執行、遞送及支援、監督
企業功能	財務報告	資訊技術	應用系統及 IT 的發展	資訊技術	資訊技術
預期的使用者	外部查核人員	管理部門、使用者、查核人員、系統開發者	顧客、系統開發者、評估者	管理部門、使用者	管理部門、使用者、查核人員

資料來源：Fredric，2002

在一般公認審計準則（General accepted auditing standards, GAAS）外勤工作準則第二條指出：查核人員應對內部控制取得充分的瞭解以規劃查核，並決定測試之性質、時間和範圍。主要關切內部控制的理由－「財務報告之可靠性」，如果影響財務報告可告性之控制不適當，則財務報告有可能無法正確地反應一般公認會計原則（General accepted accounting principle , GAAP），查核人員就無法確定財務報告是否允當表達。而 COBIT 主要是資訊技術的環境下以控制及審計的觀點為出發點，較適合於查核人員針對企業的資訊技術內部控制做評估。

（三）資訊技術之風險管理

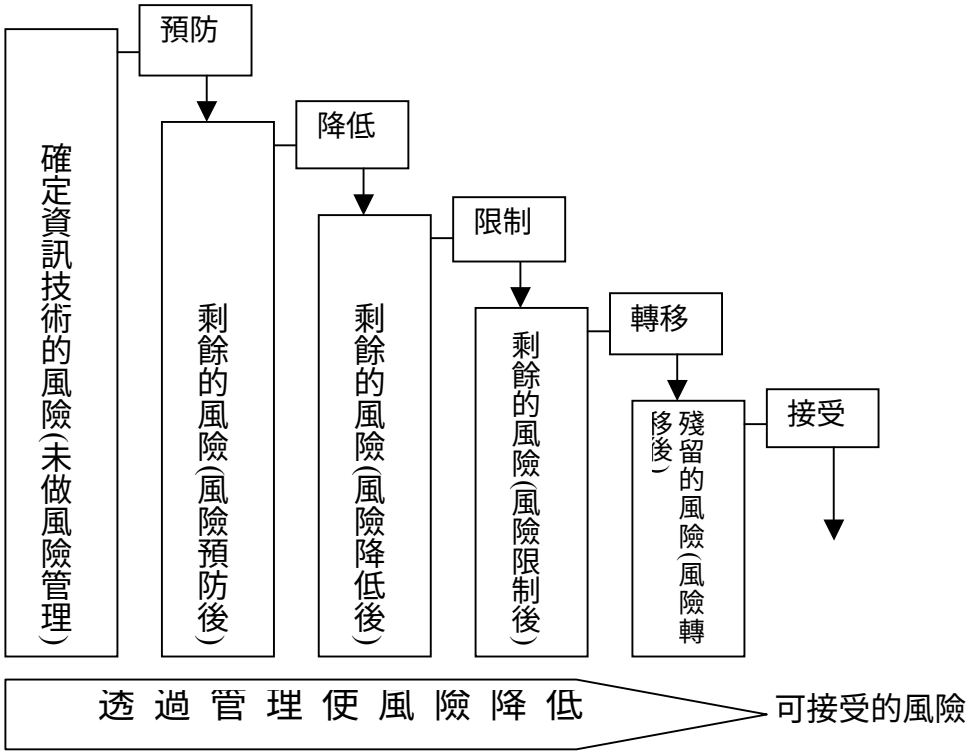
Markus Gaulke（2002）提到有效的資訊技術管理已經是企業成功的主要因素之一，資訊技術的風險管理是一個不斷的循環過程（如圖十五）。



圖十五、 資訊技術風險管理循環

資料來源：Markus Gaulke，2002

在一系列的風險管理程序後，最主要的目的就是要達到資訊安全的風險最小化（如圖十六）。若資訊技術的管理制度建立的很完善，不但可以控制成本、節省時間，更可達到企業的目標。



圖十六、 風險降低步驟

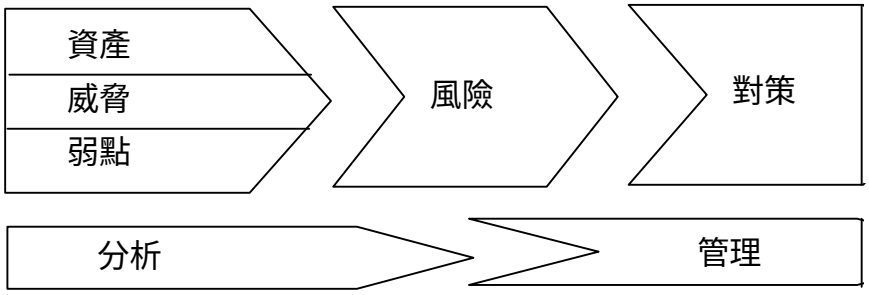
資料來源：Markus Gaulke，2002

（四） 內部控制

由於電腦技術的進步，使企業之結構產生重大的變化，企業幾乎全面升級為電子化企業，過去的管理模式已不再適用，造成企業之營運管理面臨重大的挑戰，使得內部控制更相形重要。在傳統的集權管理模式裡，通常將責任加諸於經營管理者身上，並要求對各自的部門進行控制管理，因此而造成各種弊案發生，如：金融機構的超貸、企業的財務危機、掏空資產等。而如今的電子化企業除了舊有的內部控制問題，與電子資料處理相關的風險更扮演著多數現今公司的營運危險。因此，企業的內部控制制度範圍更應涵蓋資訊安全的管理，以建構完善的內部控制制度。

蒐集相關文獻進行網路風險管理與安全控制，以確認一般風險管理模式。資訊安全風險管理的方式，隨著資訊的發展，而其使用與操作環境的演變也有所不同。Wright（1999）將資訊安全的風險管理分為三個時代(如參考文獻中所列)，其中網路服務環境特別著重於整體資訊系統的建置，所面臨的威脅型態更是屬於全方位的攻擊，因此需

由整體資訊系統的安全性加以考量。Caelli, et. al,（1989）將一般風險管理方式列示如下：



圖十七、一般風險管理模式（資料來源：Caelli, et al., 1989）

網路安全之弱點辨認與分析：

對於資訊安全弱點的分析，亦是資訊安全風險管理重要一環。通常，弱點是與威脅是並存的，因為如果對資訊安全的威脅處理越好，則其弱點也就越小；反之，若無法有效將威脅降低，則對資訊安全的弱點就越大。表四為 Caelli 等提出之資訊安全弱點分析：

表四、資訊安全的弱點分析

管理因素	人員因素	設施因素
．對於資訊安全缺乏理者的支持。 ．無效的安全組織及護措施 ．無效的風險管理 ．內部管理鬆散 ．缺乏足夠的監察程序 ．不安全的文件控管程序 ．缺乏足夠的恢復程序 ．操作程序的缺乏 ．對於意外事故計畫的不足 ．缺乏足夠的系統及端存取程序	．缺乏足夠的安全訓練警覺 ．不忠心或不可靠的職員	．不安全的環境 ．無效的錯誤偵測機制 ．不安全的應用軟體開發 ．對軟、硬體的缺乏維護 ．不安全的軟體接收程序 ．過時的軟／硬體 ．不安全或不可靠的通訊方式 ．無效的實體存取控管程序

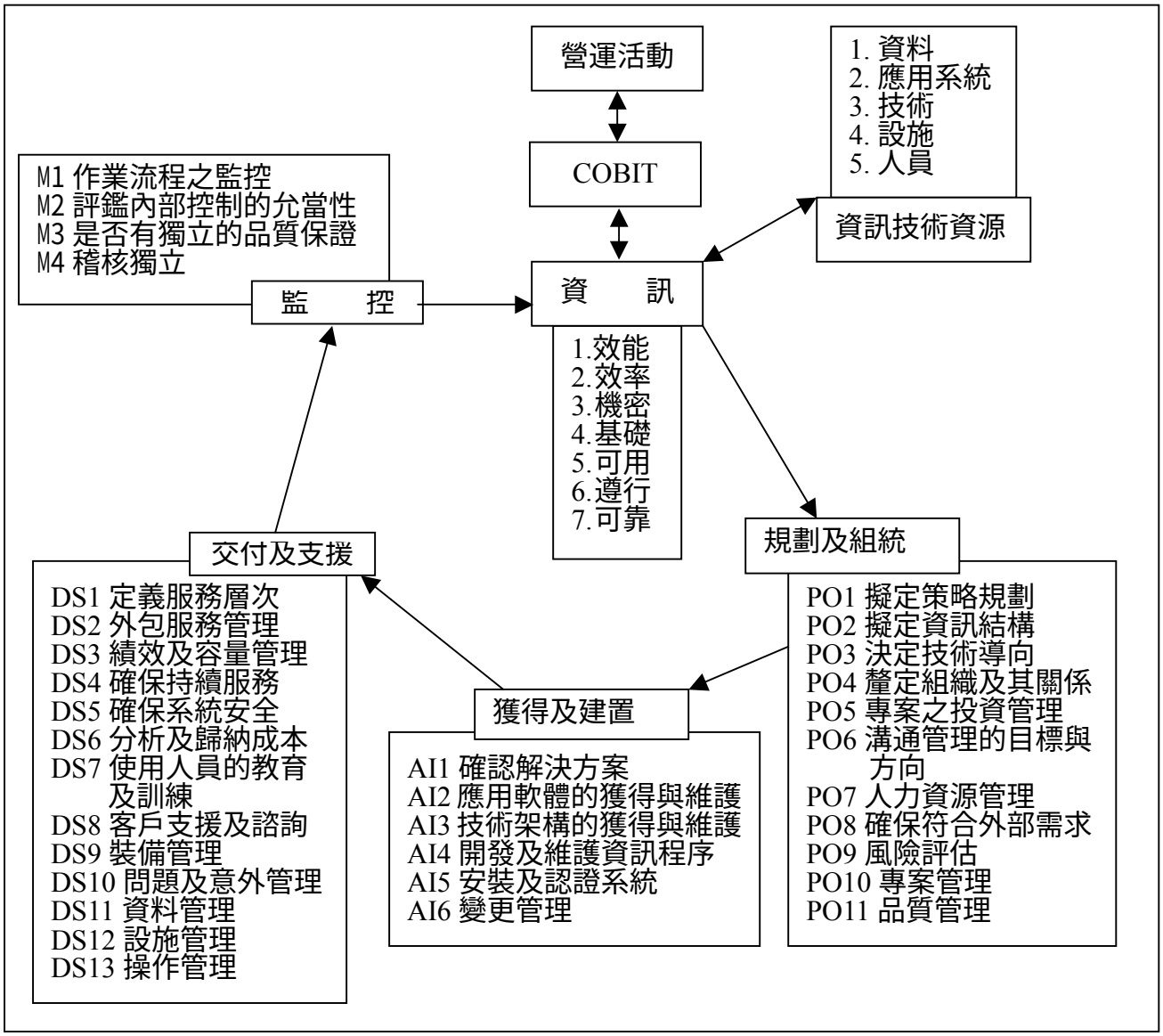
（資料來源：Caelli, et al. ,1989）

三、研究成果：

（一）採用權威性安全標準，初步建立資訊安全政策與稽核要點：

本計畫先比較現行資訊安全管理標準。資訊安全政策已有的規範有：1.「資訊及相關科技控管目的」(COBIT)；2. 英國資訊安全管理標準－BS7799；3. ISO17799；4. VISA；及 5. 其它資訊安全文獻等。本計畫嘗試藉由 COBIT、BS7799、ISO17799 等資訊安全管理規範結合資訊安全風險管理，評估各類資訊安全政策是否符合網路服務之需求與同步稽核系統之聯結，進而剖析同步稽核時，組織可適用之資訊安全政策。

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，「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，依最佳作業實例而訂定，可將控管與營運目標緊密聯結。COBIT 資訊技術安全控管之整體架構，如下圖所示：



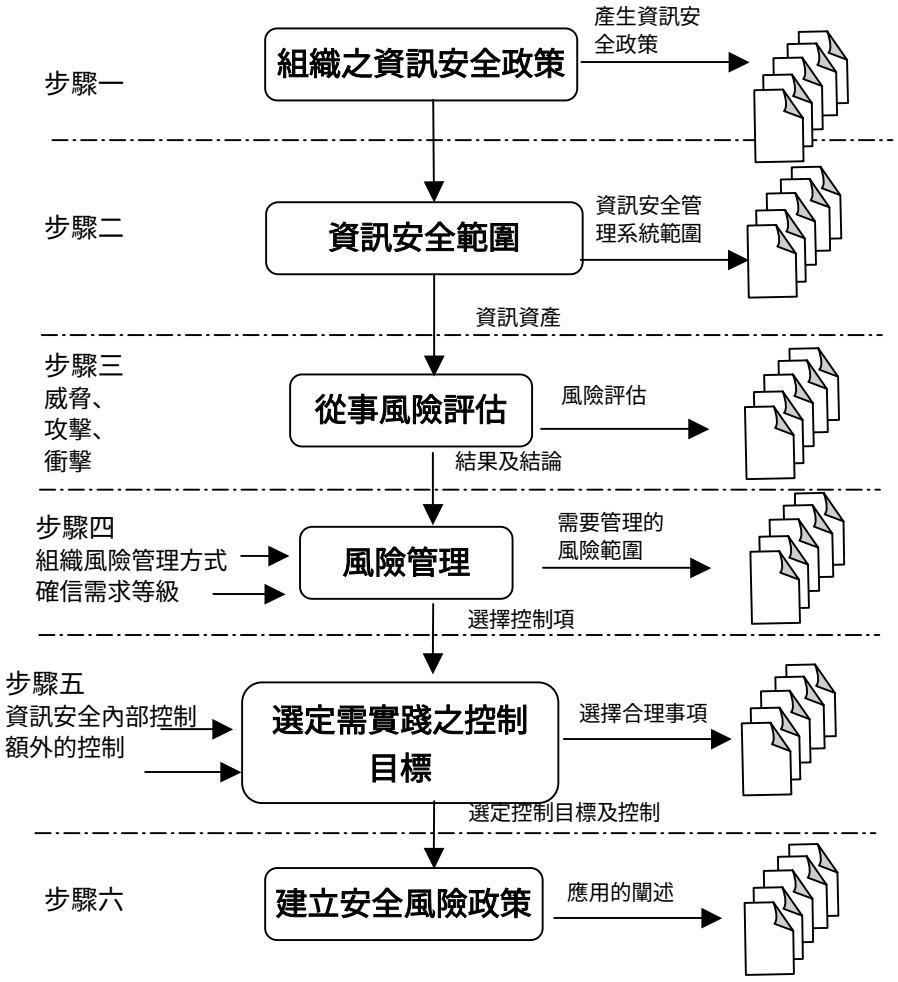
圖十八、COBIT 資訊技術安全控管整體架構（資料來源：COBIT 3re ed.）

其他如 BS7799（針對 127 項資訊安全風險評估項目建立風險等級）、ISO17799 與

VISA 等亦有類似的安全政策及架構。BS7799 第一部份皆已在 2000 年 12 月 1 日成為 ISO/IEC17799 國際標準[2、12]。而資訊安全管理在國內尚處於啟蒙階段，且在訂立這些標準時，Web Services 才剛剛崛起，這些安全政策與架構並未完全考慮開放式環境中的網路威脅與入侵，因此有必要在網路服務的環境下，重新檢視這些資訊安全標準與政策之可行性。

（二）網路資訊系統安全之風險控管模式與步驟：

建立資訊系統安全的規劃，除了考量成本、控制與便利性的考量外，在系統架構上，為防範各項入侵威脅，必須設計各項系統安全的防護技術與資訊科技管理控制。本研究之資訊系統安全之風險管理政策如下：



圖十九、資訊系統安全之風險管理實施步驟[12]

一個組織之資訊安全風險管理模式，雖經過計畫、辦認、分析及產生對策等相關程序的評估與執行，但是仍然需要對整體過程予以檢查、稽核與再評估，使能瞭解其管理模式是否符合組織使用。為了驗證本計畫之系統的應用架構，是否能應用於同步稽核資訊系統中，本計畫預計提出一個關於電子業網路服務之測試案例，以瞭解網路商務稽核之安全制度，以及實際作業需求。可對本計畫所提出風險控管政策加以改善，

以達實際可用之境地。

伍、結論與貢獻

本計畫預期之**結論與貢獻**如下：

（一）建立網路服務下的安全機制，以支援同步稽核資訊系統之應用及其導入程序：本計劃探討 Web Savices 環境下，配合 HTTP 與 Web Security 等各項機制，設計一套適用於 B2B 電子商務環境下的網路安全稽核系統架構, 此稽核架構可使會計師不再受制於受查客戶異質環境之影響，且由於稽核安全機制的發展，可支援更具功能的同步稽核資訊系統，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）可以提供審計人員明瞭ｅ世代審計專業服務的發展方向：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。因此本計畫透過研究會計師事務所資訊安全業務的現況調查，並深入探討同步稽核架構之安全性議題，可提供後續研究者在進行同步電腦稽核研究時的啟發。

（三）實作網路服務（Web Services）下之安全介面，以支援同步稽核目標之實現：本計畫設計 Web 環境下資訊安全所需的基本介面與標準資料, 可作為有意發展同步稽核資訊系統者之參考。目前 SOAP 的標準上並沒有提供任何安全可靠的保證，因此，我們藉由此計畫提供學術界一個具安全可靠機制的 SOAP 標準。經由我們實做研究雛形(prototype)的經驗，提供業學界一個後續研究發展的平台。使用本計畫所設計之稽核資訊安全介面，可強化受查客戶資訊部門對稽核資訊系統之信心，且能更進一步達成高階電腦查核與安全控制目標。

（四）在實務領域上的貢獻為提供一個支援會計師事務所稽核的資訊安全風險管理模式，且符合網路服務特性且充分整合的系統規格及藍圖：本計畫透過對目前廣泛採用的資訊安全規範進行詳細且深入的了解，可將這樣的經驗提供給會計師界及尚未建立資訊安全管理組織的參考，並將安全風險區分成不同等級，因此組織可依其預算、人力，實施相關對策，以避免人力、物力的浪費，有效管理資訊安全。

（五）可加強專業人員的訓練，提高參與人員專業知識： 對於參與本計畫之研究人員，我們預期將可獲得以下之訓練：

1.認識同步稽核架構雛型及理論。

2.對系統分析與建構安全可靠系統之能力。

3.對於 SOAP 技術能有更進一步的了解。

4.除了 SOAP 之外，對其他與 SOAP 有相關之技術能夠有一定程度上的了解，例如：WSDL、UDDI 的相關訊息以及其他 Web Services 的運用狀況等等。

5.由管理層面上，了解訊安全之控管政策的重要性。

參、重要文獻彙總

一、中文部分

1.國家資通安全會報技術服務中心，「政府機關資訊安全問卷調查」報告，http://www.icst.org.tw，2002 年。

2.黃亮宇，資訊安全規劃與管理，松崗電腦圖書，台北，1992 年。

3.行政院研考會，TCSEC 資訊安全標準評量表， http://www.Rdec.gov.tw/ipcs/，2001 年。

4.劉國昌、劉國興，資訊安全，儒林圖書公司，台北，1995 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.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。

8.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。

9.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。

10.林鳳儀、汪進揚，紀東昀“ 由電子化財務報表探討連續性審計之可行性 “ ，致理學報，第 16 期（民國 91 年 11 月），pp.187~202

11.賴溪松，「資訊安全國家標準」，資訊安全通訊，第四卷，第四期，29 頁，1998 年。

12.劉永禮「BS7799 資訊安全管理規範建構組織訊安全風險管理模式之研究」，元智大學工業工程與管理研究所。

13.黃亮宇，資訊安全規劃與管理，松岡電腦圖書，台北，1992 年。

二、英文部分

14.2001 Information Security Services: A Competitive Segmentation and Analysis, http://www.idc.com.

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.American Institute of Certified Public Accountant, “Auditing in Common Computer

Environments", AICPA, New York, 1995.
18.American Institute of Certified Public Accountant, "Auditing with Computers", AICPA, New York, 1994.
19.Allen Julia H., "The CERT Guide to System and Network Security Practices", Addison-Welsey, 2001.
20.BS7799-1, Information Security Management-Part1：Code of Practice for Information Security Management, British Standard Institution, London.,1999.
21.BS7799-2, Information Security Management-Part2：Specification for Information Security Management Systems, British Standard Institution, London.,1999.
22.Caelli, W., D. Longley and M. Shain(1989).Information Security for Managers, Stockton Press, New York.
23.Carmichael, D. R. J. H. Willingham, and C. A. Schaller, "Auditing Concepts and Methods-A Guide to Current Theory and Practice", McGraw-Hill, 1996, 6th ed.
24.Chirillo John, Hack attacks denied - a complete guide to network lockdown, 2001.
25.Donaldson Mark, "Inside the Buffer Overflow Attack: Mechanism, Method, & Prevention ", http://rr.sans.org/code/inside_buffer.php
26.Finne,T.,Information Systems Risk Management：Key Concept and Business
27.Fraud & Security, February, 9-12,1999.
28.Gibbs T. E., and R. G. Schroeder, "External Auditor Criteria for Evaluating Internal Audit Departments", *The Internal Auditor*, pp. 34-42. Dec. 1980.
29.Information System Audit and Control Foundation, "COBIT-Audit Guidelines" 2nd Edition, April, 1998.
30.Groomer, S.M. and U.S. Murthy, "Continuous Auditing of Database Applications: An Embedded Audit Module Approach", *Journal of Information Systems*, Spring 1989.
31. Halliday, S. (1996) , ''A Business Approach to Effective Information Technology Risk Analysis and Management'', Information Management & Computer Security, 4/1, 27-28.
32.Kalakota Ravi, & Andrew B. Whinston, "Electronic Commerce; A Manager's Guide", Addision Wesley, 1997.
33. Ko Calvin, Paul Brutch, Guy Tsafnat, Jeff Rowe, Karl Levitt "Advanced Security Research Journal" NAI Labs Volume IV, Number I, Winter 2002
34.Lin Fengyi, Deron Liang, Soushan Wu "Electronically Auditing EDP Systems – With the Support of Emerging Information Technologies", *International Journal of Accounting Information System*, 2001.
35. Lin Fengyi, 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.

36.Parker, D.B. Information Security in a Nutshell, Information Systems Security, Spring, 1997,16.

37.Process, Computer & Security, 19, 3, 2000, 234-235.

38.Software Architectures. *IEEE DISCEX II vol. II*. Jun. 2001.

39.Subramanya, S.R., Lakshminarasimhan, N. Computer viruses. *IEEE Potentials*. Oct.

40.2001.Visa Account Information Security Standards," visa.com/nt/gds/standards.html(2000).

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

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

43.Stasiak, k. "Web Application Security", IScontrol ,Vo1 6, 2002.

44.The ISO 17799 Service & software Directory, The Benefit of：Security Risk Analysis , 2001. http://www.iso17799software.com/riskben.htm.

Wright, M., Third Generation Risk Management Practices, Computer

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

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

48.Wright, M,"Third Generation Risk Management Practices", Computer Fraud & Security, February,9-12.,1999.

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