RDEC-RES-090-013（委託研究報告）

電子商務風險與管理

行政院研究發展考核委員會編印
中華民國九十一年六月

RDEC-RES-090-013（委託研究報告）

電子商務風險與管理

受委託單位：財團法人成大研究發展基金會
研究主持人：趙健明
協同主持人：賴溪松、 林清河 、(蔡耀全)
研　究　員：林建明、 羅維毅 、 陳宜儉
研 究 助 理：葉俊麟、(張榮庭)、(賴俊澤)

行政院研究發展考核委員會編印
中華民國九十一年六月

目　次

表　次

圖　次

提　要

一、研究目的：

本研究擬篩選國內外指標性電子商務網站風險管理措施（如電腦稽核、簽章認證、智慧 IC 卡應用等）及其實施經驗，整理其管理現況案例分析結果，根據本研究定義之電子商務交易的六大核心系統架構，及網際網路線上交易必備四項功能，利用危機預防與偵測觀念，結合風險管理的理論，發展一套電子商務網站風險管理資訊系統架構，建置風險認證、風險估計、風險管理策略規劃及其安全管理機制評估四大模組，設計網站安全風險管理雛形系統，透過對指標性電子商務網站模擬與分析作業，掌握、防範與處理電子商務網路之安全風險管理，據以編製電子商務風險管理評量表，及推算電子商務管理之平衡評量表，以提供金融業實行電子商業保險作業的參考，再根據網路資訊安全基礎架構管理之原則，具體建議健全我國電子商務風險管理制度。

電子商務風險管理是電子企（商）業發展及永續經營的一個重要金鑰，其主要功能是利用有限之資源，透過電子商務基礎系統架構之再造工程，透過施行風險辨認分析、災害衡量評估、安全防範機制與再生學習程序，將危機轉化為轉機的管理作業，此項轉化過程，實際上係利用電子商務建構之資訊系統模組，在電子商務組織各階層運作的交易與服務流程，包括瀏覽、採置、付款、配送等商業行為，藉由網際網路的系統安全機制，由遠端自動化且有效率化執行，相較於傳統面對面交易方式更快速正確且風險較低。

本計劃深知電子商務（E-commerce）係電子企（商）業（E-Business）的一部份，電子企（商）業強調經營結構的改變，而電子商務強調的則是交易模式的改變。因此，本案研究重點在於電子商務所定義之電子交易的核心架構，風險管理系統，從生產端至消費端，完整的網際網路線上交易機制與系統，建置包括：訂單管理、交易處理、付款處理、配送管理、庫存管理、客戶資料管理等風險管理系統，並為因應

風險管理各種可能的需求，建立一個具擴充性、穩定性、安全性及執行效率化的金流與物流、商流與資訊流的網際網路安全交易機制。

二、研究方法：

本研究擬利用危機預防與偵測的觀念，結合風險管理的理論與知識管理應用，發展一個電子商務風險管理資訊系統架構，內容以電子商務風險管理機制的架構為主體，並細分為風險辨認、風險估計、風險管理策略規劃及安全管理策略評估四大模組。透過各模組間的相關配合運作、掌握、防範與處理電子商務風險，據以完成風險管理評量表（e-CRSC，e-commerce risk score card）及保險作業指標，俾能進一步達成電子商務風險管理建議書。

研究過程以電子企業流程再造(e-BPR，e-business process reengineering)之應用為主題，在風險辨認與風險分析的模式中，選定故障模式與影響分析(FMEA：failure mode and effect analysis)來作為風險管理的分析方法，並探討電子商務交易系統失敗的因素及對應之預防策略，最後完成電子商務風險管理。

本研究假設電子商務改造工程（e-BPR 專案）組成元件為：（1）訂單管理系統、（2）交易處理系統、（3）付款處理系統、（4）庫存管理系統、（5）物流配送系統、（6）客戶資料管理系統；此皆為完成電子商務網站不可或缺的元件，而此專案組成元件要能完成下列線上交易必備四項基本功能：（1）查詢功能、（2）訂貨功能、（3）付款功能、（4）配送功能。

採用故障模式與影響分析方法（FMEA）做為風險辨認的工具，任何造成上述四項功能的中斷、錯誤，皆視為電子商務網站可能失敗的因素，在風險辨認階段，本研究以問題的方式採用魚骨圖（fishbone diagram）表示方式，供系統操作表點選，建構 FMEA 故障分析表單及 e-BPR 風險辨認清單。

根據上述風險辨認分析清單及故障分析表單，分析失敗因素對改善電子商務關鍵目標：成本、品質、服務與速度，所造成影響的程度，作為關鍵性指標之評量。依據各指標之強弱資訊化的狀況，與相同或

異業電子商務成熟度與資源需求等方面的比較與評析，可以構建電子商務網站之電子商務風險管理評量表（e-CRMS），此風險評量表可供實施電子商務網站, 強化系統安全結構, 與人力技術訓練的改進參考。

如果將上述風險管理分析與評量的結果，融入電子商務網站的網際網路資訊中心（IDC）的風險管理資訊系統（RMIS, risk management information system），再與電子商務網站的附加價值（EVA, economic value added）、資金流通（cash flow）及客戶滿意度、業務處理變革程度等指標，可以編製掌握電子商務網站現況經營管理之平衡評量表（EC-balance scorecard），進而引進電子商務實際執行成效評估, 則國內銀行金融業可依照國際巴賽爾銀行監理委員會（BIS）於 1998 年發表“金融業進行電子銀行與電子貨幣活動之風險管理宣言”向財政部金融局建言，督促銀行公會成立“電子商務金流作業研究推動專案小組”推動電子商務風險保險業務，以利電子商務之發展與流通。

本計劃建議採用最佳實踐法（best practice），將電子商務各經營者納入風險管理服務中心的學習組織內，建立風險管理主管團隊（chief risk manager council, CRMC），另建立風險管理資料庫共享的資訊架構，學習最佳風險業績（bench marketing）經營手法，就風險管理服務中心（risk manage service center, RMSC）之網際網路資料中心（IDC），分享學習組織團隊內最佳實踐法的風險管理技巧與手法，自己內部發展，或委外獲得最低成本的外部永續經營稽核評定與保險契約服務。

三、研究發現：

電子商務保險環境必須靠政府及企業等多方的配合，才能把此電子商務保險的機制建立起來，其中政府更扮演著關鍵的角色。政府應該致力於電子商務保險的基礎建設, 如相關政策與法令的建立, 此外, 政府也是一個最佳紛爭解決的仲裁者。

國內於十月初，第一張電子商務保險單獲准開辦，這是電子商務保險機制的一大突破，將可吸引其它保險業者跟進。當然保險業者也可參酌政府所許可的保單項目及國外電子商務保險內容，然後創新並

增加自己公司新的產品。

此外，政府應該積極鼓勵保險業者或資訊安全業者開辦此業務，例如從降低稅率或公益宣傳，讓全民都能了解電子商務保險的優點，進一步增加消費者對電子商務網站的交易信心。

由於網際網路無遠弗屆，跨國性電子商務紛爭或風險問題應值得注意。在審核保單時是否只考慮自身國情，或違反其他國家法律等，這在審查階段必須有專業的法律團隊一起檢視。另外，國外電子商務線上紛爭處理仲裁變通機制 (Online ADR) 的引進，亦可進一步建立交易仲裁機制，來達到責任歸屬的目的。

到底誰最有資格辦理此項保險業務，檢視我國目前的保單，尚未針對網際網路或是因應新興科技而設計，未來應是保險公司可以發展的空間。然而缺少精算資料、請求的頻次與數據，所以保險公司在定價部分是比較困難。另外，保險公司也會考慮到是否可以再保分擔風險，以目前全球電子商務保險尚在起步階段來看，全球的承保能力都是非常有限的。然而，經營電子商務及新興科技運用，產生許多不確定的風險，也不同於以往保單所承保的標的，企業多利用合約來減少或降低自己的風險，如果能再加上商業保險機制的運作，相信會更有助於電子商務的推動。

保險業者在缺乏精算保費基礎之下，可以串聯成立資訊安全部門，來衡量各種資訊安全上的風險，此外，也可以參酌國外的保單政策，來設計自己的產品。另外，資訊安全業者也是適合經營電子商務保險的公司，因為他們是最清楚資訊系統漏洞的地方。

最後就獨立的電子商務保險(stand-alone E-commence insurance)內容說明，包含傳統第一人險及第三責任險的部份：

（一）第一人損失險，其內容有：

1. 標準軟、硬體財產損失險
2. 潛在電子資產實體損失險
3. 潛在資訊財產的損失

4. 潛在小型犯罪險
5. 潛在綁架勒贖險
6. 個人及廣告的損失

（二）第三者責任險，其內容有：

1. 標準商業責任險
2. 智慧財產權的侵犯
3. 潛在電子商務專業險
4. 潛在電子商務媒體險
5. 商業收入及額外支出

不幸發生損失或者遭破壞的時候，透過保險機制的運用，能從電子商務保險取回部分的補償，減輕或者是分散消費者及電子商店的責任，對於電子商店或者是消費者都會有所保障。

四、研究建議：

為了要達到上述電子商務風險管理目的，首先必須建立起適當風險管理環境，這裡所謂的風險管理環境，是指國家資訊基礎建設應包括下列兩項機制：

（一）電子商務風險管理中心：

此管理中心同時也是風險稽核單位，用來辨認和評估風險程度，並建議適當風險趨避措施。

（二）電子商務保險機制：

無論多麼周全的電子商務網站，仍然必須承受新科技不確定風險。電子商務保險機制將是降低此不確定風險的好方法。

首先，就電子商務風險管理中心而言，我們建議建立一個服務電子商務的機構—電子商務風險管理中心。由政府核定一個公正的電子商務評鑑機構，該機構對欲申請優良商店標章的電子商店進行各項標章的評鑑，在評鑑合格之後，電子商務評鑑機構將授予該電子商店優良商店之標章，以取得消費者的信任。而電子商務風險管理中心負責

提供欲申請優良商店標章的電子商店相關的服務，例如幫助該電子商店規劃設計，以符合優良商店標章的內容，順利通過電子商務評鑑機構的評鑑，取得優良電子商店的標章。

建立電子商務風險管理中心的目的在於服務電子商店，使消費者對電子商務更有信心，增強消費者利用網路來消費的便利性。對於幫助電子商店成為優良電子商店的目標如下：

1. 提升電子商店服務品質經營水準：

   針對各業種業態服務人員，進行服務技巧專業訓練，使得服務員不致於因系統操作錯誤而造成交易雙方損失。並且進一步導入企業內應用，藉以提升商業整體服務技能、服務水準，強化經營競爭力。

2. 強化電子商店服務品質意識：

   與 ISO 精神結合，以利內部品質稽核觀念與精神真正落實於企業內部管理中，達到國際共同規範。

3. 塑造電子商店全面顧客滿意新形象：

   結合多方面力量，擴大優良商店作業規範（GSP）認證標章之認知度及知名度，讓社會大眾能清晰、簡單的認識優良商店（GSP）之優點，塑造商業服務業全面顧客滿意新形象。

此外電子商務風險管理中心也具有電子商務風險管理的服務，且可幫助電子商店仲介投保電子商務險，使得經過電子商務風險管理中心協助過的電子商店能夠贏得顧客的安心、信賴及滿意，建立成為一個環境好、衛生好、制度好、服務好、經營好的電子商店。綜合電子商務風險管理中心所提供的服務主要有以下四點：

1. 提供優良商店標章服務：

   電子商務風險管理中心對於想獲得優良電子商店標章的電子商店，只要該電子商店對電子商務風險管理中心提出申請，電子商務風險管理中心就會幫助該電子商店規劃設計。設計該電子商店變

成一個能夠通過評鑑機構對優良電子商店之標章所需評鑑的各個審查項目(欲獲得標章所需達到的標準)的電子商店，也就是代表電子商務風險管理中心會幫助該電子商店規劃其內部設計，使得該電子商店能夠成為達到優良電子商店標章安全水準的電子商店，夠資格取得優良電子商店標章的優良電子商店。

2. 提供電子商務風險管理的服務：

電子商務風險管理中心能夠對電子商務網站做以下的評估及服務：

- ◆ 基本軟、硬體及系統風險的評估。
- ◆ 網路弱點的評估。
- ◆ 資料相關風險評估。
- ◆ 掃描電子商店在網路操作上安全的弱點。
- ◆ 第一人損失和第三者的責任風險的評估。
- ◆ 生命週期損失控制的服務。
- ◆ 指示電子商店如何建立自己的網路安全和電子商務損失控制機制。
- ◆ 定期傳送病毒資訊及損失控制的服務。
- ◆ 附加技術服務，幫助電子商店取得或維持一個安全的電子商務環境。

3. 提供交易雙方身份認證作業：

電子商務風險管理中心應該提供電子交易買賣雙方的身份認證作業，有助於在執行電子商務交易時，彼此身份確認，且有交易不可否認的效果。

4. 提供代理電子商務保險的事宜：

電子商務風險管理中心能夠幫助電子商店代辦電子商務保險（包括電子商務保險的內容及諮詢），使得電子商店能夠透過電子商務風險管理中心的服務，對於適當的項目投保電子商務險，其中

包括第一者損失險及第三者責任險。其次，就電子商務保險制度而言，電子商務保險應具備哪些功能及特性，我們就三個角度來探討：購買者角度、販賣者角度、以及執行電子商務交易者角度：

（1）購買者角度：

電子商務保險的最大功能即是降低網站經營者的風險。這些風險無奇不有，包括病毒攻擊或第三者入侵所造成無法營業的損失、或是資料的損壞。其次，員工的不忠誠或是不可避免的犯罪行為介入也是風險來源。另外，網站經營者誤用別企業的專利或商標、智慧權的侵權行為，亦是不可預知的風險。

（2）販賣者角度：

過去產險產品並不適合使用在電子商務站經營上，因為電子商務經營有其獨特的風險內容。因此，保險公司若只販賣傳統的產物保險，將無法吸引電子商務業者去購買。就經紀人而言，推銷這些商品將是事倍功半。另外，過去層出不窮的保險條文紛爭也造成保險業者與保險者之間的困擾，保險者近期也都更進一步檢視保單詳細條文，對於含糊不清的產物保險，保險者是退避三舍態度。對於電子商務保險而言，電子商務風險明訂於保險條文，將會吸引更多相關資訊產業經營者的進一步青睞。相對保險公司而言，公司創造出新產品，有助於公司業績發展；同時，因為明文規定風險範圍，也有助於責任的釐清。

（3）執行電子商務交易者角度：

電子商務保險除了第一人責任險外，一般還包括第三人責任險。所謂第三責任險是包含電子交易執行者所蒙受損失的賠償問題。第三人可以是交易的顧客、上游供應商或其它社會大眾，當他們在執行交易引起糾紛時，電子商務保險可以確認責任賠償的問題。如此，可讓交易雙方都有風險上保障。

綜合本研究計劃各項工作項目的完成，最終可以整理健全我國電子商務風險管理制度之具體建議報告。其短、中、長期目標之詳細說

明，如下頁表所示。

健全我國電子商務風險管理制度之具體建議表

時程	具體建議政策與措施	主辦機關/協辦單位	參考備註
短程：	(1)培訓各公私機關資訊部門資訊安全長。	經濟部主辦，研考會協辦。	
	(2)成立電子商務風險管理服務中心。	經濟部主辦，財政部協辦。	
中程：	(1)成立電子商務評鑑機構(公正第三者)。	經濟部主辦，公平交易會協辦。	
	(2)成立電子商務店驗證組織。	經濟部主辦，消基會協辦。	
	(3)推動電子商務保險機制。	經濟部、財政部主辦，消基會協辦。	
長程：	(1)建議電子商務風險管理中心及保險機制納入國家資訊基礎建設範疇。	經濟部、財政部主辦，交通部協辦。	
	(2)促成電子商務風險管理中心以國家組織的方式積極參與 CIS (the center for Internet service)為國際性非營私公司組織(cooperative organization)標章服務工作(charter service) 。	經濟部主辦，外交部、消基會協辦。	

第一章 前言

第一節 基本定義說明

一、電子商務的定義背景

電子商務是「泛指一切透過網際網路所完成的商業行為」。換言之，在網際網路的平台上利用電子數位訊息的交換，從上游的原料及資訊提供者、製造及編輯組合商、中間銷售商到終端使用者間所有的交易行為，交易商品內容亦包含了所有支援與服務性的工作。透過電子商務的機制，消費者的購買行為從搜尋、訂購、付款到取得商品與服務，所有的活動過程都在網際網路線上協助完成。

本來商業活動的目的是滿足消費者的需求，電子商務經由網際網路的連接，消費者以電子通訊快速的方式取得所需的產品，所以原料及資訊的供應商、製造商、中間銷售商及消費者之間的溝通過程更為順暢，商品資訊及配送路徑資料的傳遞完全地電子化，因此，電子商務也可說是「生產端至消費者的完全電子化」。

（一）電子商務所造成的商務改造工程

電子商務使得多數傳統商務市場的限制釋放而不存在，例如商家所在的地點及環境並不影響經營效益；換句話說，在網際網路的平台之上是一個完全開放的市場，而且這個市場正逐年快速的成長。如果從產業活動的演變來看，電子商務所代表的是一項新興的商業革命，不僅改變了交易活動的模式，對市場也產生相當大的衝擊與改造，包括：通路的改變、交易活動成本降低、數位產品的興起、產業結構的改變、企業資源的重新分配等。

此外，由於網際網路是一項快速、便利的工具，消費者可以輕易的找到所需要的產品資訊，在消費市場具有主導權，所以市場機能從製造供應端的生產導向、中間商的銷售導向、已經轉變為消費端的顧客導向的服務機制。更因為網際網路的無

遠弗屆，電子商務市場可說是全球性的市場，跨國性的購買行為也在彈指之間就完成了。電子商務所造成的改造工程如下詳述：

1. 通路的改造

在傳統的商業活動中，大多數的商品並非直接由生產者銷售給最終的使用者，而是仰賴中間商的參與，將商品銷售到市場，在這個活動中參與的成員所組成的集合就是所謂的「行銷通路」（marketing channel）。最簡單的通路結構就是由生產者和消費者所組成。但是為了接觸更多的消費者及潛在消費者，製造商大多委託中間行銷機構銷售其產品，例如：批發商、經銷商、零售商...等。隨著商業活動的發展，生產者要將產品更精確的銷售給所需要的消費者，必須仰賴完整的通路結構，因此通路結構更趨複雜化。

但是由於網際網路的普及，電子商務的應用改變了複雜的通路結構。經由網際網路的連線作業，「網路」（network）可視為一種新型態的通路，製造商只需將產品型錄放置在「網頁」（webpages）上，購買者即可在電腦螢幕前透過瀏覽器迅速的取得完整的產品資訊，進行線上購買，縮短通路階層。

2. 交易成本結構的改造

（1）搜尋成本：

消費者只需透過電腦螢幕簡單的點選操作，即可輕易地瀏覽網路上所有的商品供應店家，找尋所需要的商品，節省到處尋找的時間成本。

（2）價格成本：

價格會反映成本，當商品經由行銷通路由生產者傳至消費者，每一個環節中或多或少會產生商業利益，消費者所需付出的價格成本也因此累計。透過電子商務的應用，消費者進行購買時可以越過幾個中間

商進行，交易價格也因此降低。

3. 數位化商品與數位現金的興起

一般而言，電子商務雖然存於虛擬的網路世界，卻是架構在實體世界的商業市場，進行交易的商品是為了滿足消費者的需求，所販售的商品也是存在實體世界。但是由於資訊科技的進步，許多商品都可以經由數位化處理後在網際網路傳輸，例如：電子報、MP3、線上教學、軟體下載、資料庫檔案...等，這是應用電子商務興起市場所產生的新商品。此外，為了在網路上進行交易，新興的付款工具如：數位現金、虛擬信用卡、電子支票...等也應孕而生。

4. 產業結構的改造

電子商務造就了一個新興的虛擬市場(virtue market)，在市場的運作模式中，原有的參與者被排擠時，其所提供的服務機能將被新興的產業所取代。舉例來說，當消費者欲進行線上交易時，必須透過網際網路服務供應器(internet services provider；ISP)，才能連上網際網路，為了迅速找到所需的商品，必須借由入口網站（portal site）的協助。而繼續存在的傳統產業為了迎應市場的變動，也必須進行再造工程，因此，產業結構已由勞力密集、資本密集轉向資訊密集。

此外，由於線上購物人口的增加，消費金額成倍數成長，商店業者如何將產品精確、快速地交到消費者手中，則必須仰賴完善的物流配送業來服務，因此，電子商務的發展亦帶動了物流配送業的成長。

5. 資源的重新分配

電子商務對企業所造成的影響還包括資源的重新分配，商品在以往的銷售模式中，為了增加商品的曝光機會及接觸更多的消費者，企業通常投入大量的人力、物力在銷售前端的作業，諸如：業務銷售人員的配置、零售點的設置，

但是以電子商務的運作而言，銷售前端將只是電腦螢幕所呈現的網頁畫面，企業必須將前端資源轉換為後端支援系統，包括：資料處理人員、系統維護人員，線上諮詢服務（call center service）等。

一但企業導入電子商務系統，將以更少的人力完成更多的工作管理，能夠輕易地掌握企業的營運情況，簡化的作業流程及統一的庫存管理，使得企業經營更具效率。

6. 電子商務潛在的風險

由於電子商務改造傳統交易方式，並以快速電子化的資訊傳遞，因此，在各階層運作的過程，如從訂單管理、交易處理、付款處理、配送管理、庫存管理、客戶資料管理等電子化資訊系統中，無疑亦衍生前所未有的安全風險，如何從網際網路中建構一套網站資訊安全管理系統是值得深入探討之課題。

7. 風險管理

風險管理是一項十分複雜的工作，在瞬息萬變的網際網路世界中，許多企業內在與外在的因素都是我們難以控制的，因而風險管理也逐漸受到企業的重視。

（1）風險管理的技巧

在發展電子商務與推動企業 e 化的過程中，企業會遇到許多的障礙。不論硬體、軟體或人員，企業都必須清楚的瞭解潛在的失敗因素，並利用有效的策略來降低風險。每個企業都應該根據其企業文化經營型態，制定屬於自己的風險管理機制，而一般最基本的風險管理概念包括：

- 評估執行的成本與效益，並藉由多種解決方案來降低風險。

- 評估做與不做之間的風險，而不只是要怎麼做的問題。
- 評估對企業的影響，有效分配內部資源與外部資源來執行工作。
- 建立符合知識經濟時代的企業組織，減少人為的風險。
- 評估技術的延展性，建立穩固的技術基礎。

（2）風險管理的步驟

風險管理包括確定、評估與管理三大步驟：

- 確定風險：

  風險包括人事、需求、技術、商業等複雜的組合。找出可能的潛在風險，就是風險管理的第一步。

- 風險評估

  要評估電子商務與企業 e 化的風險十分困難。一般來說，可以藉由顧問或有經驗的人獲得，定期評估可以有效防止潛在的風險，而不會等到事態嚴重時才發現。

- 風險管理

  預防風險最好的方法就是妥善地準備、定期地評估、溝通與改善，也是降低風險的不二法門，而有效的知識管理策略更是預防風險的利器。

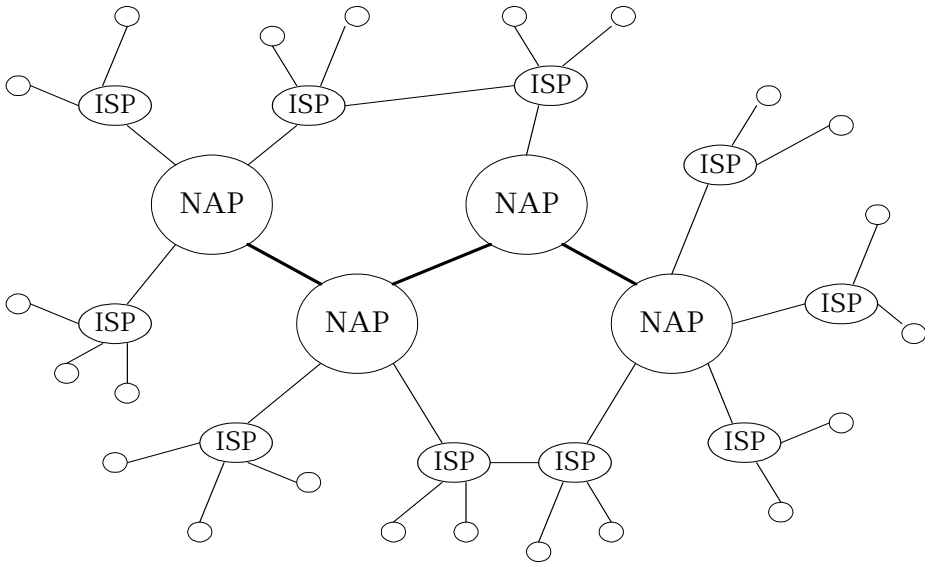
第二節 作業標準及協定

一、資訊流

（一）網際網路架構

網際網路目前為一超過三萬五千個相互連結的網路所構成的網路系統。在交互連結的網路間所含括的有：(1) 可達國際各國的相互連結骨幹。(2) 存取／遞送之次網路，以及 (3) 數千萬個連結各種組織伺服器的私有及公共網路，並含有許多大家感興趣的資訊。該骨幹乃由網路服務提供者運作（network access points），包括 MCI、Sprint、UUNET／MIS 及 BBNPlanet 等公司。任何一個骨幹每月皆可處理超過三百兆位元以上的資料，遞送之次網路乃由地區及區域性網際網路服務提供者（ISPs）所提供；而 ISPs 與 NSPs 在網路存取點（NAPs）上進行資料交換。Pacific Bell NAP（位於舊金山）及 Ameritech NAP（位於芝加哥），皆為此種類型的交換點範例（Minoli,1998）。圖 1 提供一對於 ISPs、NAPs 及骨幹間交互連接的高層次觀點。

圖 1- 1 網際網路之架構

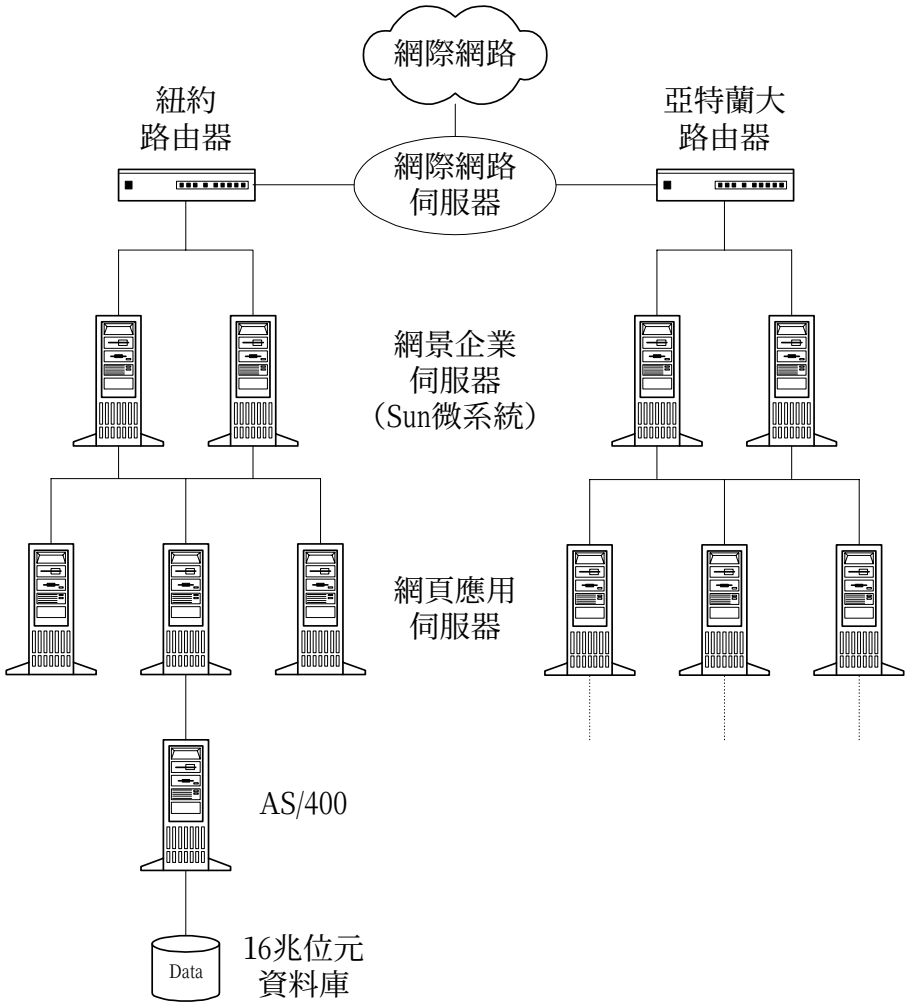


資料來源：參考書籍 R2（八）

當使用者自其電腦發佈一項申請於網際網路上，則該申請將很可能通過 ISP 網路，並行經一個（或以上）之骨幹，且跨越另一個 ISP 網路，到達包含感興趣資訊的電腦；對申請的回

應也將遵循一相似的路徑。對任何給定的申請及其對應的回應，並沒有預定之行程。事實上，這些申請與回應皆各自被分割為小封包（packets），而且這些小封包可依循不同的路徑。這些小封包所行經之路徑由路由器決定，該路由器具有可更新網際網路上網路地圖的機制，如此可決定小封包通過之路徑；思科（www.cisco.com）為高速路由器的首位提供者。

圖 1- 2 UPS 的網路架構



資料來源：參考書籍 R2（八）

（二）網際網路通訊作業標準及協定

網際網路運作的問題是如何建立一系列作業標準及協定，國際義務性組織 IETF（The Internet Engineering Task Force, http://www.ietf.org/ ）有責任發展網際網路規格及標準。

通訊協定乃指決定兩電腦間如何透過網路與彼此通訊的法則，環繞於網際網路設計之協定內嵌一系列設計法則：

1. 可相互操作性：

系統支援來自不同供應商的電腦與軟體；對電子商務而言，此代表顧客或企業無須再購買特殊之系統來進行業務。

2. 層級化：

網際網路協定之集合乃以層級方式作業，各層級乃架構於較低階層級之上。

3. 簡易性：

架構中的各層級僅提供部分功能或作業，此代表應用程式乃隱身於複雜的硬體架構之下。

4. 終端對應終端：

網際網路乃建構於終端對應終端的協定之上，代表資料的解釋乃由應用層進行（即寄送與接收端），而非於網路層。這與郵局的作法相當類似，郵局的任務為遞送郵件，只有寄出者與接受者知悉其內容。

用以解決全球網際間的問題為傳輸控制協定／網際網路協定（TCP/IP）。此乃代表任何連向網際網路的電腦或系統皆採行 TCP/IP，這也是電腦與系統所唯一共同享有者。事實上，如同表 1-1 所示，TCP/IP 為兩項協定——TCP 與 IP，而非單一項。

TCP 乃確保兩電腦間可以在可靠的狀態下相互通訊。各 TCP 通訊在接收後必須加以回應，倘若其間通訊未於一合理時間內做出回應，則發出資訊之電腦必須再遞送輸出資料。電腦要能夠發出一項申請或回應給網際網路上另一部電腦，則該項申請或回應必須分隔成小封包，並標記發出及接收電腦的位址；這也就是 IP 所參與的時機，IP 乃將小封包予以格式化，並指定其位址。

現今的 IP 版本為第四版（IPv4），在此版本下，網際網路位址有 32 位元之長，而且以句點分隔四串數字的形式表示，如 130.211.100.5；此格式亦稱為點記四分定位法。在網際網路上你可能熟悉如 www.yahoo.com 位址，在這些類似英文的位址後面，乃為 32 位元的數字化位址；而該數字化位址是由網際網路資訊中心（InterNIC）所指定。

表 1- 1 TCP/IP 架構

應用層（FTP, HTTP, Telnet, NNTP）	
傳輸層	
傳輸控制協定（TCP）	使用者數據協定（UDP）
網際網路協定（IP）	
網路介面層	
實體層	

以 IPv4 的方式，可採用的最大位址數超過四十億個（即二的三十二次方）；乍聽之下，這可能是個很好的數字，尤其網際網路上的電腦仍僅數百萬部。但位址並非各地被指定，而是採分區方式；例如，當惠普（HP）公司在數年前申請一位址時，其即被指定起始區塊為 15 之位址，此代表惠普公司可以自由指定超過一千六百萬個位址給網際網路上的電腦，範圍由 15.0.0.0 到 15.255..255.255。較小的組織則被指定較小範圍之位址區塊。

雖然區塊指定減少了路由器所須進行的工作（例如：如果一位址開頭為 15, 則其可知將連向 HP 網路的一部電腦), 但此即隱含現有可用的位址數可能在未來幾年內不敷使用。基於此項因素, 各類的網際網路團體委員會於 1990 年代初期, 即開始起草新一代之網際網路協定 (IPng)。此協定（稱為 IP 第六版, IPv6）正開始運用 128 位元之位址, 此將允許一千兆部電腦（十的十五次方）連向網際網路。在此機制下, 每個家庭將有自己的網路, 而這些家庭網路除了家中電腦外, 尚可就具有自身特定位址之各類型應用系統加以交互連結與存取。

（三）網際網路安全

安全性通常被視為電子商務的主要障礙, 例如：預期的使用者戒慎恐懼於網路上傳送信用卡資訊；而預期的銷售者擔心網路駭客將侵略其系統。雖說加強安全性的需求乃為一企業邁向「交易導向」的電子商務, 然而即使是行銷網路都難免擔心安全受侵犯而遭受傷害。國家電腦的安全協會（NCSA）指出四項安全電子商務的基石, 包括：

1. 確實性：

指訊息的寄送者（客戶端或伺服器端）為其所聲稱的身分。在 TCP/IP 中驗證一使用身分的基本方法乃為密碼, 但密碼是可以臆測或攔截的。網際網路協定位址亦可加以視察, 以避免未受核可的存取行為；然而 IP 仍無法驗證小封包確實為來自某特定網域。利用一種稱為 IP 電子欺瞞的技術, 網路駭客可以寄送看似來自某特定網站, 但實則不是之訊息、或更改一網頁上的 URL；如此後續的存取仍可進行, 因為其看似受一具公信力的網站所看管, 但實則不然。

2. 隱私：

訊息的內容受到保密, 而且僅為寄出者與接收者所知。違背隱私權的情事可能在傳輸時或傳輸後發生。一旦訊息被

接收後，寄出者必須確認其內容仍具有隱私性。在此，內容一詞乃指其廣義精神。舉例而言，當使用者自一網站存取一個網頁，關於交易資訊的進出記錄乃被建立；進出記錄包括時間、日期、使用者機器位址及使用者前一次參觀網站的URL。倘若使用者透過 ISP 進行網頁存取，ISP 伺服器將潛在地保留使用者所參觀的每個網站。同理，許多商業網站使用特殊類別物件來保存使用者的資訊。在大部分的情況中，有特殊類別物件乃正當合法地被運用。然而，部分廣告業者以不道德地使用特殊類別物件追蹤使用者查閱的習性；最大的威脅並非資訊被以秘密的方式取得，使用者大方地提供給網站的資訊可能才是最危險的。

3. 完整性：

訊息的內容在傳輸過程中不可被修改。TCP/IP 以純文字方式傳輸資料封包，由於與特定訊息相關的各封包，當其由客戶端移向伺服器端再送回時，通常經過許多路由器及線路。在路由器內時，他們很可能被擷取或修改。例如，駭客可以修改成為一張表單內容在提出申請時所送達的地址，使用者可能在一張表單上填具信用卡號碼，並點選「申請」鍵，即可能在無知的情下將資訊傳送給駭客。

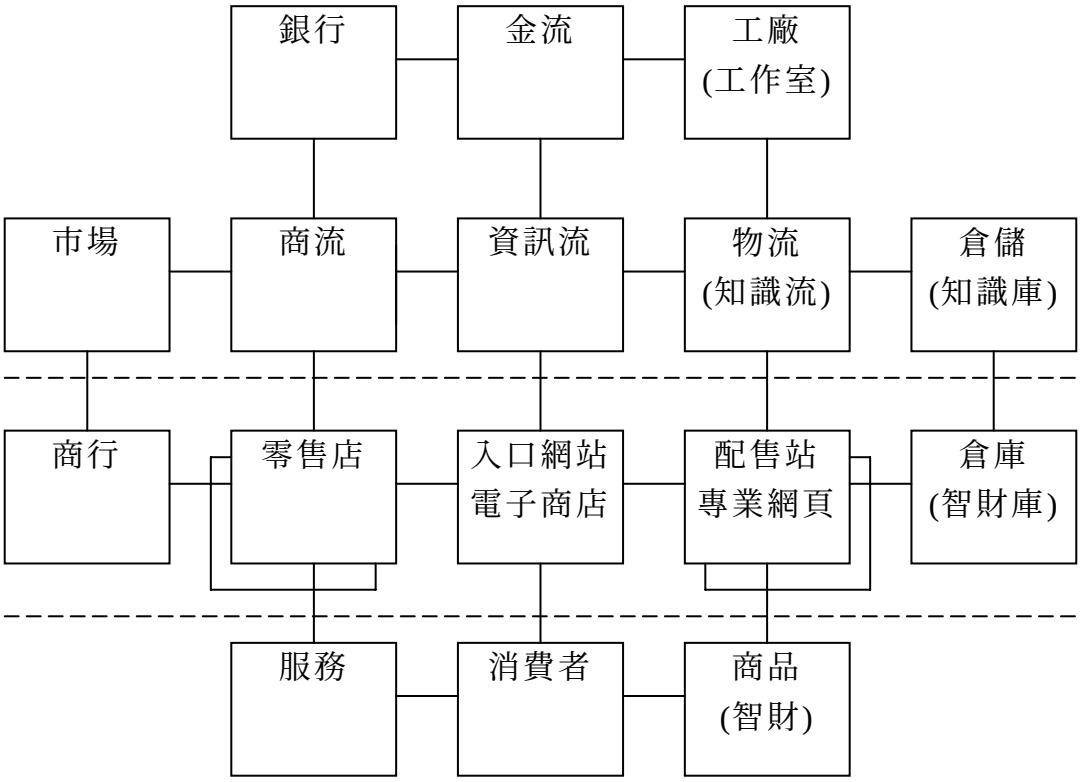
4. 不可否認性：

訊息寄送者無法否認寄送訊息的事實。倘若你透過郵件訂貨型錄訂購一項貨品並以支票給付，之後即很難爭辯該訂單的事實性。如果你透過電話號碼為 1-800 之型錄訂購的相同貨品，並以信用卡給付，之後則總是有爭議的空間，雖然電話識別號碼可以用來釐清該訂單發出的電話。相似地，可以使用網路型錄即信用卡付費，之後你絕對可以辯稱並非你發出該訂單；雖然伺服器所建立與更新之存取記錄檔會自動記錄寄送者網際網路位址。不可否認性的關鍵在於簽名機制，這可以使你所涉及的交易不容易引發爭議。

簡言之，一個電子商務網站要安全保密需要這些基石先予以安全保護。狹義而言，此代表資料與資訊的隱私必須受到保護，身分必須被驗證及具有可驗證性，而未受到核可的存取必須加以控制。要確認一個電子商務網站全然地安全是件相當複雜的任務，當中有一些指導原則，如 Stein（1998）及 Garfinkel 與 Spafford（1996）文中所提及。在下一章（第二章），述說保密安全解決方案：如加密、數位簽名、驗證與防火牆，並提供在一電子商務應用系統中客戶端與伺服器端安全的基石。

第三節 電子商務整體架構

圖 1- 3 電子商務整體架構圖



一、電子商務之四大功能

（一）查詢功能

1.商品查詢

提供完整電子型錄，含實體圖像、產品相關資訊，如店內條碼（in-store marking)、原印條碼（source marking）及報價供消費者瀏覽，並可經由簡單的蒐尋引擎協助消費者獲得所需相關訊息。

2.訂單查詢

提供消費者經由線上進行交易，下單訂購並隨時上網查詢訂單的處理狀態及交易紀錄。

（二）訂貨功能

1.訂單資訊：

提供購買者於訂單確認前，能檢視訂購產品型號，數量及價格的表單，即一般常見的「購物推車」。

2.網路下單：

提供消費者經由線上直接點選，完成訂貨程序表列訂單訊息，內容包含交易雙方之基本資料、相關日期、訂貨項目明細及總計金額，與雙方電子簽章等資訊。

（三）付款功能

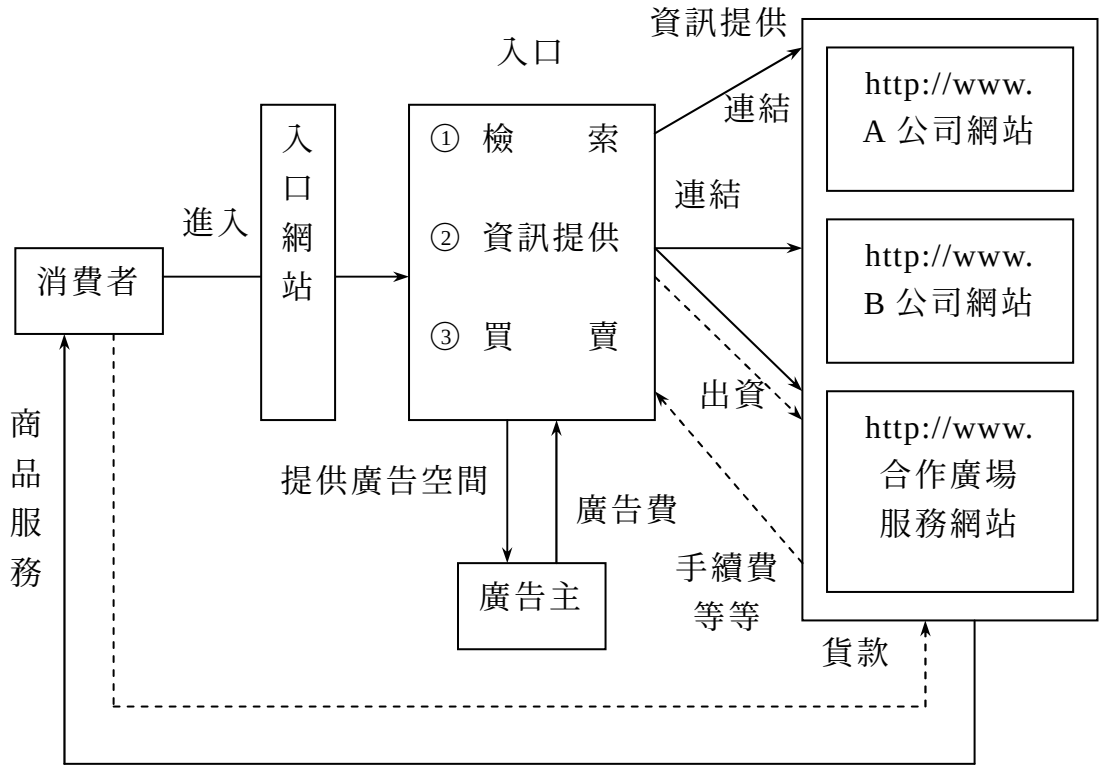
提供消費者線上付款的機制，接受包括：信用卡、電子現金、電子支票、金融 IC 卡等數位付款工具的支付，直接經由網路線上完成交易。現行支付一般係透過網路銀行（Internet banking）信用卡、轉帳卡，金融卡、授權銀行自動扣帳、SET、SSC 轉帳等方式施行，並在特定時間點上，提供相關之對帳單，說明交易帳務狀態資料。

（四）配送功能

提供消費者採購時，商品運輸、配送及代收貨款等服務，及採用最快速路徑，經供應商配售站，實體運送商品到消費者處，應提供配送條碼（dispatch marking）及託運單供消費者上網查詢配送情形，亦需一併提供消費者簽驗商品及託運送回覆單後之退換貨的售後服務與運輸配送服務。

二、電子商務之入口網站

圖 1- 4 電子商務入口網站（PS）系統架構圖



電子商務之入口網站（portal site），是指當顧客在網路上要尋找所需商品和服務時，首先進入的網站。最具代表性的入口網站就是能夠提供各種資訊的檢索網站，和各個供應者架設的首頁網站；另外有一些公司針對其特定的商品和服務，設置各式各樣的

入口網站讓顧客使用，也算是典型的入口網站之一。一般而言，這些入口網站所提供的資訊，多半是基於使用者的興趣來加以分類，而這種分類的結果，往往能夠直接反應使用者的實際需求。一個公司或企業若善加利用這些特色，並且讓製造商和仲介業者直接與入口網站連結的話，就可以產生新型態的網際網路事業。

目前這種網路事業的重要趨勢，就是各企業之間以入口網站為核心，由相關業者合作成立商品和服務的綜合性網站，而彼此合作的範圍，從汽車銷售業者之間的合作，到旅行社業者和地圖公司之間的合作都有。另外，一些企業與消費者（business to consumer）的交易，例如在入口網站上直接處理結帳業務，或是直接處理自由市場拍賣（free market auction）等等，現在也成為一個新趨勢。此外，在資訊仲介（infomediary）逐漸成為商業趨勢的今天，別處無法得到的詳細資料，也可以在此獲得滿足，於是類似像「destination」這類的網站就應運而生。若要說代表的例子，在美國可以說是雅虎（Yahoo）、MSN Network、AltaVista、美國線上（AOL）與 Netscape 等網站；至於在日本，則是以 ISIZE 最具代表性。

三、電子商務之六大核心系統

電子商務之六大核心系統架構圖如圖 1-5 所示：

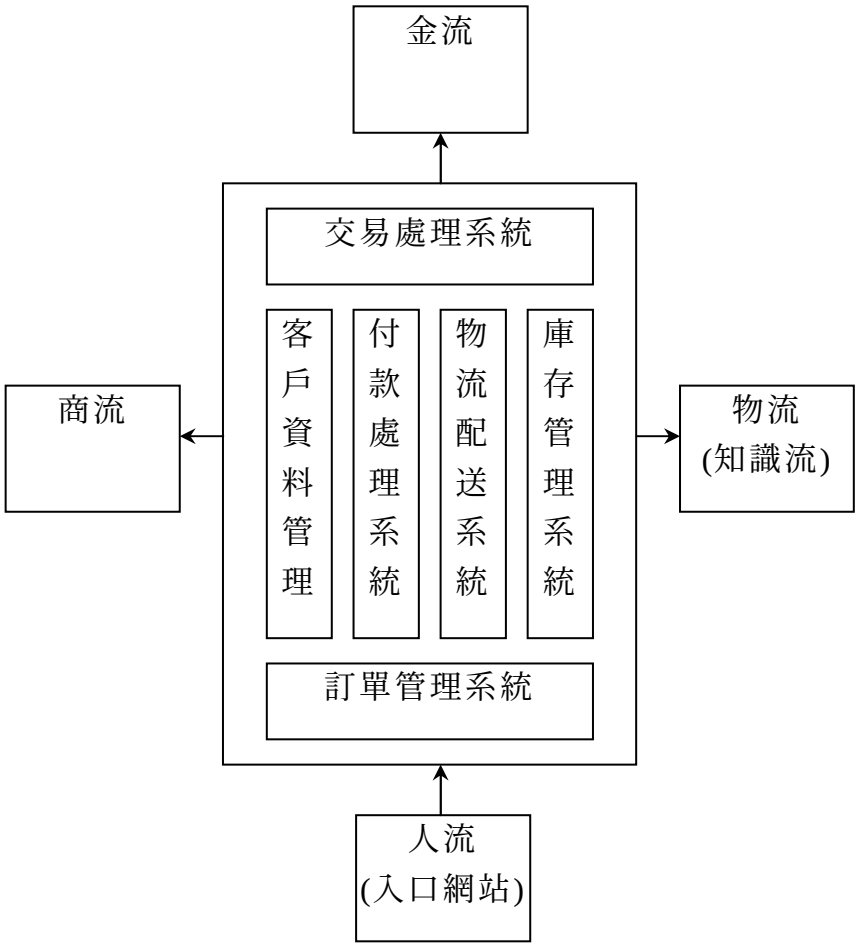
（一）訂單管理系統

訂單管理系統是電子商務的第一件核心系統，消費者經由入口網站台（PS）檢索，連結電子商務站後，由線上商品查詢、訂單查詢，決定下單訂貨至完成訂貨程序前後，提供消費者完整訂單訊息。主要訂單產生後，按物流、付款、庫存及客戶系統之需求，拆開訂單訊息，其內容應包含交易雙方之基本資料、相關日期、訂貨項目明細及總計金額等，傳送交易處理系統進一步總合處理，並產製訂單回覆單供消費者查詢訂單處理狀態及交易記錄等。

所以訂單管理系統的機能在於掌握經營的情況，完整的訂

單管理系統可以供商家做為銷售分析，了解商品的銷售情況、營運收入、業績表現，從訂單資料還可以做為行銷決策分析，將熱門商品、促銷商品、乏人問津的商品做不同的銷售計劃，因此，訂單管理系統是經營者的決策支援分析工具。

圖 1- 5 電子商務之六大核心系統架構圖



（二）交易處理系統

交易處理系統是電子商務的主要核心系統，其功能在透過電子資料將訊息即時傳遞至相關的供應商及配送商，從顧客送出訂單、商家確認訂單、送貨、收款的流程管理，商家隨時能

由線上查詢了解該筆交易進行的階段。譬如：一但訂單確立後，同時將送貨資料傳遞至物流中心通知送貨，供應商、庫存中心也即時得到相關的補貨訊息，所有的進行過程必須能由交易處理查詢系統得知。

因此，完整的交易處理系統也可以說是供應鍊管理（supply chain management，SCM），從訂單的處理、訂貨、供貨及帳款的收付情況都在系統的管理範圍。此外，當線上同時間的交易量增加時，是否有能力同步處理是系統設計必須考慮之課題。基本上交易系統與訂單系統配合，利用資訊系統共享的設計原則，可以迅速的整合付款、物流客戶及庫存系統等資訊，實現JIT（just in time）新型態的經營，也即是「無庫存、無資產」與「重視資金流向」的企業經營方式。

（三）付款處理系統

電子商務系統為了能在網路上完成線上付款行為，必須具備付款處理系統，所接受的付款工具必須是多樣的選擇，以應付不同消費者的需求：供應商、配送商間 B2B 系統所處理的是企業之間大筆金額的支付，自然不適用信用卡交易，因此必須透過企業與金融機構簽訂的轉帳付款作業約定，如 SET、SSC 轉帳等；若是一般的交易，則使用電子現金、信用卡、金融 IC 卡...等支付工具。隨著網路交易行為日趨頻繁，處理線上小額付款的微處理機制也是必要的功能。

然而種種付款處理方式最重要的仍是「安全」問題，若是金錢透過網路傳送過程缺乏安全的保障，則線上交易風險大，而且交易的機能就不算完整，電子商務的發展也勢必受到限制。所以，線上金融交易的風險管理是整個電子商務風險管理的核心。

（四）庫存管理系統

經營一家網路商店的前提就是無店鋪（虛擬店鋪）的銷售活動，所以過多的庫存量是不必要的浪費，而且在網路商店所

販售的商品種類項目可能持續地增加，要達到低庫存量、甚至是零庫存的目標，必須透過庫存管理與供貨廠商建立快速供貨系統。否則經由無店鋪的銷售模式所減少的成本，卻支應在後端龐大的倉儲及存貨成本，豈不本末倒置。

庫存管理系統處理商品資訊，應以商業自動化所訂定之製造及銷售使用之消費者單元（comsumer unit）之原印條碼（source marking）與店內條碼（instore marking），雖無實體商品之庫存，但是已保用交易契約的商品標的物。「商品條碼」及「契約附加碼」，才不至淪為買空賣空。

（五）物流配送系統

當顧客透過線上交易完成商品的訂購，除了智財數位產品可以經由線上傳輸完成商品的交付外，仍必須藉助實體的運送服務將商品送交至消費者手中，因此與物流配送業者的聯繫管理顯得格外重要。當消費者選擇在網路上消費，其目的不外乎是要求快速的交易服務，如果取得商品的時間過於冗長，將不能滿足消費者的需求。

因此，應與集訂單處理、倉儲管理與檢貨配送資訊於一身的「物流中心」合作，訂定「快遞」配送系統的策略聯盟服務，保證滿足消費者對於時間的需求。

（六）客戶資料管理

電子商務終極是顧客主導式的交易活動，所以顧客是商家最大的資源，運用電子商務技術能夠進行一對一雙向的溝通，與顧客建立良好的互動關係。由禮遇優良顧客，提供符合個別顧客的服務，可以增強商場的競爭力。

客戶資料安全的維護是建立顧客信賴的第一步，經由消費記錄分析，可以了解消費者的消費取向，進行顧客化的商品推薦，也可以依消費者的不同需求提供服務。一般而言，吸引一位新的客戶所需花費的成本是留住一位既有客戶的 5 倍，所以

新世代的經營哲學不僅是提高顧客滿意度，更應該建立顧客的忠誠度，因此，客戶資料管理系統（customer relationship management，CRM）的應用顯得格外重要。具體而言，不只要收集客戶的資料，亦要活用這資料庫，並透過各種客戶管道收集資訊，依據客戶各自不同的需求加以區分，適時提供符合客戶個別需求的商品設計，提昇客戶購買誘因。不只能保有舊客戶，亦可以開拓新客戶。

第二章 風險類別與管理

第一節 知識管理之應用

電子商務風險管理是電子企（商）業發展及永續經營的一個重要金鑰，其主要功能是利用有限之資源，透過電子商務基礎系統架構的再造工程，施行風險辨認分析、災害衡量評估、安全防範機制與再生學習程序，將危機轉化為轉機的管理作業，此項轉化過程，實際上是利用電子商務建構之資訊系統模組，在電子商務組織各階層運作的交易與服務流程，包括瀏覽、採置、付款、配送等商業行為，藉由網際網路的系統安全機制，由遠端自動化且有效率化執行，相較於傳統面對面交易方式更快速正確、無風險。

本計畫深知電子商務（E-commerce）係電子企（商）業（E-business）的一部份，電子企（商）業強調經營結構的改變，而電子商務強調的則是交易模式的改變。因此，本案研究重點在於電子商務所定義之電子交易的核心架構－風險管理系統，從生產端至消費端，完整的網際網路線上交易機制與系統，建置包括：訂單管理、交易處理、付款處理、配送管理、庫存管理、客戶資料管理等風險管理系統，並為因應風險管理各種可能的需求，建立一個具擴充性、穩定性、安全性及執行效率化的金流與物流、商流與資訊流的網際網路安全交易機制。

本研究擬利用危機預防與偵測的觀念，結合風險管理的理論與知識管理應用，發展一個電子商務風險管理資訊系統架構，內容以電子商務風險管理機制的架構為主體，並細分為風險辨認、風險估計、風險管理策略規劃，及安全管理策略評估四大模組。透過各模組間的相關配合運作，掌握、防範與處理電子商務風險，據以完成風險管理評量表（e-commerce risk score card，e-CRSC）及保險作業指標，俾能進一步達成電子商務風險管理建議書。

研究過程以電子企業流程再造(e-BPR，e-business process reengineering)之應用為主題，在風險辨認與風險分析的模式中，選定故障模式與影響分析(FMEA，failure mode and effect analysis)作為風險

管理的分析方法，並探討電子商務交易系統失敗的因素及對應之預防策略，最後完成電子商務風險管理。

本研究假設電子商務改造工程（e-BPR 專案）組成元件為：(1) 訂單管理系統、(2) 交易處理系統、(3) 付款處理系統、(4) 庫存管理系統、(5) 物流配送系統、(6) 客戶資料管理系統，而此專案組成元件要能完成下列線上交易必備四項基本功能：1.查詢功能、2.訂貨功能、3.付款功能、4.配送功能。

採用故障功能與影響分析方法（FMEA）做為風險辨認的工具，任何造成上述四項功能的中斷、錯誤，皆視為電子商務網站可能失敗的因素，在風險辨認階段，本研究以問題的方式採用魚骨圖（fishbone diagram）表示方式，供系統操作表點選，建構 FMEA 故障分析表單及 e-BPR 風險辨認清單。

根據上述風險辨認分析清單及故障分析表單，分析失敗因素對改善電子商務關鍵目標：成本、品質、服務與速度，所造成影響的程度，做為關鍵性指標之評量。依據各指標之強弱資訊化的狀況，跟相同或相異電子商務成熟度與資源需求等方面的比較與評析，可以建構電子商務網站之電子商務風險管理評量表（e-CRMS），此風險評量表可供實施電子商務網站，強化系統安全結構，與人力技術訓練的改進參考。

如果將上述風險管理分析與評量的結果，融入電子商務網站的網際網路資訊中心（IDC）的風險管理資訊系統（RMIS，risk management information system），再與電子商務網站的附加價值（EVA，economic value added）、資金流通（cash flow）及客戶滿意度、業務處理變革程度等指標，可以編製掌握電子商務網站現況經營管理之平衡評量表（EC-balance score card），進而引進電子商務實際執行成效評估，則國內銀行金融業可依照國際巴賽爾銀行監理委員會（BIS）於 1998 年發表“金融業進行電子銀行與電子貨幣活動之風險管理宣言”，向財政部金融局建言，督促銀行公會成立“電子商務金流作業研究推動專案小組”推動電子商務風險保險業務，以利電子商務之發展與流通。

本計劃將採用最佳實踐法（best practice），將電子商務各經營者納

入風險管理服務中心的學習組織內，建立風險管理主管團隊（chief risk manager council，CRMC），另建立風險管理資料庫共享的資訊架構，學習最佳風險業績（bench marketing）經營手法，就風險管理服務中心（risk manage service center，RMSC）之網際網路資料中心，分享學習組織團隊內最佳實踐法的風險管理技巧與手法，自己內部發展，或委外獲得最低成本的外部永續經營稽核評定與保險契約服務。

第二節 第一者風險（first-party risks）

電子商務風險比傳統風險更複雜。例如，他們在範圍方面更國際化而且產生許多未知的結果，導引第一者損失和第三者的責任風險。進一步來說，不僅第一者和第三者，甚至在那些風險之內重複的部分也很危險。下節將討論第三者的風險。在這節中，將把第一者風險分成下面這些的範圍：（1）傳統風險、（2）安全風險、（3）倚賴或者信任風險，這些風險可能是性質的破壞、資料的損害和時間的浪費，而使商業、服務中斷，增加額外的花費。

一、傳統風險（traditional risks）

傳統的第一者風險涉及了對物質和經濟的損失和損害，包括電腦硬體或其他物質上的損失等。為保護實體財產免受傳統風險之害，在建立保險財政的程式或訂定各項契約時，即應適時提出這種風險。在許多風險管理出版物中對傳統風險的處理均有詳細的介紹，例如 Risk Management and Insurance Audit Techniques, by Dwight E. Levick (Standard Publishing Corporation)。

二、安全風險（security risks）

電子商務公司所面臨的損害風險源自他們的電腦系統和電子資料。由於駭客損壞或者截取網路網址以偷取秘密資料，並且傳播電腦系統病毒，損壞公司財產或他人財產。雖然病毒經常藉由網際網路來攻擊電腦系統，但是大多數成功的攻擊來自內部，駭客攻擊典型的動機包括：(1) 財產獲得、(2) 好奇心、(3) 諜報、

（4）報復、（5）透露、（6）自我肯定、（7）分裂、（8）競爭、（9）名聲、（10）勒索。

三、安全破壞（security breaches）

安全破壞是指某公司的電腦系統或資料，未經授權即遭到盜取或是破壞的情形。例如駭客入侵公司的電腦系統裡偷取或者損毀資料。隨著網際網路擴張，電腦系統遭到侵犯的情形日益嚴重，更甚者有非故意的雇員，或者不滿的前雇員，進行偷竊行為或者損害。

由於所有商業幾乎全賴電腦日以繼夜的運作，公司的電腦或者資訊安全系統的破壞對所有商業都是一個風險。把軟體譯成密碼雖可提供某種程度的保護，但也增加另一項風險，病毒或者其他的毒蟲能損壞設備或者資料。

資訊的偷竊行為可能為對手提供一個戰略優勢，造成財政資料、顧客資訊、人員資料及市場和新產品資料等商業秘密和資料外流。資訊被盜用可能會損害顧客、雇員和商業夥伴等第三者的權益。資訊的偷竊行為將導致或引發一個公眾關係問題。一旦電腦被病毒入侵，被犧牲的將包括與該電腦連結的其他電腦，而造成彼此間的商業中斷。當某公司的資訊系統遭受外力的介入及破壞時，將損及該公司的信譽。這類安全破壞的問題已經引起國內外政府的重視。

四、駭客的面目（a look at hackers and crackers）

hackers 破壞電腦系統的原因很多，為個人營利到電腦台系統裡破壞的 hackers 稱為"crackers "， crackers 和 hackers 會造成第一責任險損害、商業的中斷和第三責任險等損失。如果它用最笨的方法去破壞或者切入" snatched"這個地點，將迫使網路管理人員關閉這個地點。hackers 也能夠破壞網站的防火牆，而 crackers 能切斷一個系統，並針對內容及目的來侵犯該資料庫，使公司遭受財政和信用受損的惡夢。東歐 hackers 不久前盜得 CD Universe 顧客的信任卡片數字並在網路上公佈出來。這類敲詐和恐怖活動對電

子商務產生威脅，商業間諜活動層出不窮。有 72%的美國高科技公司相信自己已經成為國內間諜活動的目標，其中 46%認為間諜來自外國的競爭對手，而 32%則認為是外國政府。

五、電腦犯罪的風險（a closer look at fraud and crime risks）

電腦犯罪的範圍是無限的。大多數的犯罪出自於惡作劇，例如常見的病毒或特洛伊病毒的入侵、信用卡資訊的偷竊行為和信用卡的破解、醫療保險和醫療補助的竊取、智力性質的偷竊行為、軟體的非法使用及儲備和日用品銷售的操縱等等不法行為。多數電腦犯罪側成的損失皆被保險接受，但是，如果沒有適當制定安全檢測，保險費將會相對提高。沒有充分電子安全保護的財政機構和公司將損失更多金錢、資訊。大多數公司及機構所遭受的電腦犯罪是由自己的雇員或離職雇員，神不之鬼不覺地由內部進行破壞，但是也有許多遭到外來者入侵，進行破壞和偷竊的例子。

老練的犯罪組織擅於利用電子商務技術進行犯罪，例如俄國的犯罪小組，建立加勒比海的虛擬銀行，透過網際網路洗錢。電腦恐怖活動成為政府和商業人被不滿的人勒索的新途徑，最後還可能被迫關閉工廠、發電廠、交通控制系統，甚至重要網路程式或者城市的通路。現今電子商務的帳務估計有百分之五十是信用卡的方式。有幾個信用卡服務供應者發現，有成千到數百萬信用卡的帳目資訊潛藏著詭計。參與程式的商人能夠制定自己的評等標準，依照個體帳目的信用來同意或者拒絕處理。

許多電腦相關的犯罪和欺騙，法律並沒有辦法加以制裁。敲詐是特別難解決的犯罪行為，因為公開也許會有害公司或者機構。多數公司為保護他們的形象，寧願隱瞞公司的缺點，深怕失去大眾的信賴。在網上從事電子商務的公司，希望顧客跟他們進行商業行為時，能夠感覺到安全，所以很少公開他們的損失，除非損失很大以致於他們沒有選擇才會公布。

只有使大眾相信電子商務有充分的安全時，電子商務才能夠真正普及。使用網際網路的人大多很關心網路的安全性，有些消

費者不相信網際網路的安全性，不願意在網路上留下他們的個人資料，而超過四成的網路消費者會故意留下錯誤的資料。由於不相信網路安全的人很多，因此立法加強網路安全就更為急切。為了增加顧客信心與參與，電子商務不斷提升自己的安全，以對抗網路上的犯罪。

六、破壞的手法（methods of breaches）

駭客用來存取電腦系統和資料而造成他人損害的手法很多，常見的方式包括病毒、"spamming"、網路攫取和其他人的侵入。攻擊者用病毒來影響個人電腦或者工作站時，即有意圖破壞一個作業系統或者控制程式。可能在資料中心或者對傳輸網路發送一程式或病毒，來造成系統的損害。1999 年 ExploreZip 特洛伊馬傳染了許多電腦，一旦電腦中此病毒，當使用者打開了這些拉鏈配屬傳播的病毒時，就等於執行了含有可執行的配屬鏈結文件，ExploreZip 被視為一條蚯蚓，因為它能夠在網路上其他的電腦傳播自己，只要打開視窗時，即會執行這個病毒。

另一個方法是"spamming"，入侵者利用資訊水災的方式，破壞這個伺服器或者電腦。Spamming 是駭客報復的工具，他們透過網路之間控制通訊聯繫的草案 (ICMP) "ping attack"迫使目標回應，當這些訊息大量湧入時，目標伺服器就會超載。

不久前駭客曾用「服務的分發否定技術」來攻擊世界著名且高度安全的網站，包括 Yahoo.com、eBay.com 和 amazon.com。這個技術利用假冒的資料侵犯網路上許多電腦，造成網站的資訊水災。目標網站因為工作過度且記憶體不足而減慢對真正顧客的服務速度，甚至關閉整個網站。

七、攸關風險（relevance risks）

由破解者的破壞能夠嚴重地影響到商業的行為，但破壞的行為有些不是針對商業本身，而是透過商業所依賴的另一個商業行為。例如幾乎每個商業者必需依賴電話公司，和他們的網際網路服務供應者。供應者和顧客取決於彼此的電子資料系統和互相系

統，例如第三者的日用品交易。當一個系統失敗時，它可能使得另一些系統也失效。

八、風險的效應（consequences of risks）

上述的第一者風險出現許多不同類型的損失，通常可歸為三個範圍：資產的損失或者損害、商業中斷及有形和無形的額外花費。

（一）有形資財損害（property damage - tangible property）

公司有形資財的損害是指建築物或者其他設備（包括電腦設備）的損害。在電子商務世界中，有形資產損害的焦點在於電腦網路，尤其是資料的損害。而有形資產的損害可以藉由保險來補償損失，並由法院決定是否許可投保。

（二）無形資財的損害（property damage - intangible property）

當違法者無視或涉及智慧財產權時，也可能造成資產的損失。複製版權、冒用商標或偷取他人思想和專利均是不被允許的。在今天，公司的智慧財產權也許是它最有價值的資產。公司必須保護他們的智慧財產權，避免駭客、破壞者、競爭對手或他人奪取，同時也要確保自己不會侵犯他人的智慧財產權。

（三）商業中斷（business interruption）

時間因素的損失是典型的商業中斷損失。所謂「時間因素損失」是指企業經營者在進行商業交易時，受到外力或其它因素干擾或攻擊，造成某段時間內無法繼續營業的損失。這些損失可以從過去經營績效乘以商業中斷時間而得。對電子商店網站而言，時間因素所引發的商業中斷損失是一項容易發生的風險。諸如伺服器遭受網路駭客流量攻擊、網路線路不穩定或中斷、無法判別的交易資料、資料的偷竊行為、甚至資料庫的完整性遭破壞等等，都是商業中斷損失。這類商業中斷的損失除了中斷時間內的收入損失外，恢復商業交

易的復原費用，以及對交易者信任度降低的無形損失，都是影響所及。

商業中斷不僅阻礙資料庫的操作，對系統的使用者也有影響，由於存取的資料無法判讀，資料被盜取的機率增加，將嚴重威脅到資料庫的完整性（例如信用卡資料庫的安全）。然而系統完整性是可以重建的，資料庫的所有者可以在系統方面使活動縮短直到損害估價完成。

（四）額外損失（extra expense）

商業中斷時為了迅速恢復運作，往往必須支付額外的費用，包括重新選擇伺服器操作網站的附加費用、修復損壞設備費用、重新建立流失資訊的費用。

第三節 第三者風險（third party risks）

電子商務承襲了商業必須要面對的第三者風險，包括智慧財產權和隱私權的風險。

以下將討論包括商標、版權、專利、匿名、大量廣告信、加密和E-discovery等重要的風險。此外，廣告和出版的風險、消費者保護和不公平的商業實踐風險、專業的風險也將在此一併討論。

一、智慧財產權的風險

電子商務牽涉合法且需要保護智慧的財產權有三種主要類型：商標、版權和專利。它們的概念有所重複，使多數人不了解期間的差異。事實上，在保護智慧財產權的方法有明顯的差別，分述如下：

（一）商標基本介紹

美國專利和商標辦公室把商標定義為如下：

1.商標（trademark）是一個詞、名字、符號或者用於貿易的標誌，可以表明商品的來源和區分不同商家的商品。

2.記號（servicemark）雖然類似商標，但是是用來確定和辨識服務的來源，而非商品。一般用術語「商標」和「記號」來區分商標和 servicemarks。

商標權可以阻止他人使用類似的記號，但不能阻止他人製造相同的商品，或者以相似的記號販賣相同的商品及服務。用於州際或國外的商業商標可以向專利局和有關單位註冊。" Basic Facts about Trademarks" 描述了授權商標和一般的資訊的註冊程序。

Trademark 或者 servicemark 可能是任何事物：字母、詞、標語、圖片、顏色、口號、和聲音，只要它很特殊，就能受到美國商標法的保護；如果僅僅是「描述性」或「一般」的記號則否。當使用相似的記號為商標而產生「混亂」時，該商標即違犯商品和服務的原則。法院視許多要素來判斷商標間是否有混亂的可能性，基本上會注意到他們的相似程度和各自的商品和服務。其他要素則包括商標的相對強度、消費者對商標辨識程度和公司的意圖。

商標與版權或專利的區別在於只要所有者繼續以某商標代表自己的商品或服務，即能持續保有商標保障的權利。聯邦商標註冊的期限是 10 年，每 10 年必須更新。然而，在初始註冊日期後的第五年和第六年之間，登記者必須把將註冊保護的宣誓書歸檔。如果不歸檔，將取消該註冊。

（二）電子商務和商標

商標保護是保護智慧財產權的三個方法中最密切相關的。智慧財產權和電子商務涉及大多數商標和網路網站的問題，影響了 domain names、linking、framing、metatags，和 banner。

（三）Domain Names

Domain Name 是網站的位址。Domain Name 的爭論涉及了 cybersquatters（佔據域名）和不公平的商業競爭，以及正常商

標違反和稀釋的問題。不肖業者損害 domain name 的 cybersquatters, 並以高價把 domain name 賣給商標所有者。此外, 把公司的 domain name 登記為對手公司的商標，也是不公平的商業競爭。國會已經在 1999 年年底，透過 anti-cybersquatting（反佔據域名）與 cybersquatting 建立合法的框架工程以保護消費者，在該法律下，如果有上述「壞信念意圖」的非法行為，將迫使所有者放棄該 domain name。在 In Interstellar Starship Services Limited v. Epix, Inc., 983 F. Supp. 1331 (D. Ore. 1997), 被告的 domain name 使用了原告的商標" EPIX "。法院因為被告在選擇位址時並非刻意，而且兩者的產品類型不同，判決此案沒有不公平競賽的問題。

（四）連接（linking）

透過「連接」的過程，網路使用戶可以利用圖像的超聯結從「連接頁」（原始網路網址）到「被連接的頁」，自動地傳送不同網址。「連接」對於電子商務是必要且簡單的方法，但是當它被不當使用時，便有訴訟上的問題了。例如花花公子控告某個成人網站使用它在聯邦註冊的商標，在「小兔子」、「花花公子」兩個網站之間連接。法院認為該成人網站的商標會誤導一般大眾混淆這兩個網站，判決此案有失公平競爭。

（五）版面（framing）

framing 與 linking 類似，它允許使用者轉移到其他網站。framing 是分割另一個團體站台的過程，用來展示自己透過 hyperlinks（超連接）做的廣告或者標識語。使用者能在電腦螢幕上同時看到不同的網站。framing 的使用就像 linking 一樣，牽涉許多相同合法的爭議, 包括不公平的競賽、違反廣告法等。

（六）代碼（Metatags）

Metatags 是指被寫在個體網頁裡的隱藏代碼，也就是搜尋引擎，例如 Yahoo!和 Lycos，能夠快速地掃描所有網路中的網站，以滿足搜查者的特定要求。下面是 metatags 被違法使用的

例子。1999 年 4 月 22 日 Brookfield 通信和西海岸娛樂公司控告第九個電路侵犯他們的 domain namec 和 metatage 。聯邦法令認為消費者尋找原告的網站時，可能取而代之找到被告的網站、使用被告的服務，導致「初始利益混亂」，因而初步判決被告有罪。

1977 年喀爾文使用花花公子的標籤，法院認為此舉在成年娛樂商業中有混淆之虞，結果花花公子贏得此次的官司。然而 1998 年花花公子控告他人使用「花花公子」、「性伴侶」等術語，法院則認為被告僅在描述性話題，並不會造成消費者的混淆，而判決被告無罪。

（七）廣告旗標(banner advertising)

以旗幟做廣告和關鍵字容易引發 linking、framing 和 metatagging 的相關爭議。旗幟廣告通常出現在網頁上方。當用戶點選這些廣告時，用戶會自動連接到廣告商的首頁。這也許不算一個大問題，但是廣告商靠搜尋引擎以廣告自己的商品，每當用戶在一個搜尋引擎上填入關鍵字，它的旗幟廣告就會出現，已經具有欺騙性。

二、基本版權的定義

USPTO 和聯邦法把版權定義如下：版權提供原作者的著作，包括戲劇、音樂、藝術，和其他出版或未發表過的作品一個形式上的保護。根據 USCO 和聯邦法，任何出版物一旦被創造不需要註冊即受智慧財產權保護。

版權的保護，必須符合下列條件：作品一定是原創的。版權不保護標題、名字、短片語、和口號，也不保護思想、程式、方法、系統、過程、概念、原理、發現、或者裝置。「公正使用的定義」是判斷是否違反版權的依據。下列是影響公正使用的幾個因素：

(一)使用的目的和特性

(二)版權工作的自然性

(三) 部分關於版權工作的使用

(四) 使用對潛在市場的影響或者版權工作的價值

在電子商務世界中，資料的保護是最重要的議題。使資料庫符合版權保護的範圍而受到保護時，不但可以避免駭客的侵擾也可以擁有商業和個體的優先權。凡是因商業目的，用再生產、分發版權、拷貝或抄襲的電子方法影響另一個版權的財政營利，都將造成犯罪的因素。

1998 年制定的 DMCA, 可保護線上的供應者合法發送或是儲存資料版權，在網頁聯結的「線上服務供應者」—包括個人和組織的版權責任上，增加四個新的規定，範圍涵蓋短時間通信、系統隱蔽所、個人系統或者網路方面、資訊的儲存和資訊的位置工具等。音樂工業使用電子方法盜錄或拷貝版權著作的情形很多，不但 mp3 的爭論引起許多訴訟, 傳統的新聞機構和出版商也已經涉及電子資料庫中版權著作的爭議，例如：Playboy Enterprises, Inc. v. Hardenburgh et al.，982 F. Supp. 503 (N.D. Ohio 1997)，一個佈告欄系統的操作員鼓勵他們的用戶下載某些文件，在佈告欄系統郵寄，已經違反了智慧財產權。

花花公子的另一個案例是企業網路操作員提供原告雜誌中有版權的圖像。用戶通路一不小心就會違反版權，前不久流行的 RealPlayer 和 RealNetworks 允許人們送出音頻和視頻的文件, 製造者以 Streambox 軟體破解音頻和視頻，在 RealPlayer 上玩，直接侵犯版權違反 DMCA。

三、專利的定義（patent basics）

USPTO 和聯邦法為專利定義如下：專利對發明者是一種合法的保障，根據 USPTO 規定，一定要創新而實用的發明才可以獲得專利。在美國，國會制定了美國專利法，以增進科學和有用的藝術的進步。新專利把專利的應用歸檔到更早的日期，或者視情況將歸檔日期提前 20 年。美國專利補助金僅在美國、美國領土和美國的財產內具有效力。專利品未經授權被其他人仿冒、待售、

賣到美國之外或「輸入」到美國，都是非法的。

根據 USPTO，未經許可製造、使用、待售、或者拍賣美國的任何專利的發明，都是違犯專利法。隨著 USPTO 法院正式通過軟體專利法令，專利法和電子商務是目前網路商業中最熱門的兩項議題，許多著名的公司正在為他們的電子商務和商業方法申請專利。下列列舉這些公司所申請的專利：

(一) Amazon.com ： 在網路上使用信用卡的系統。

(二) 公開市場：線上廣告。

(三) Cybergold：在網路上看廣告會有獎勵的辦法。

(四) Priceline.com：允許消費者購買飛機票。

(五) Netcentives：線上購物方程式。

(六) Holdings, Inc：在線上支付時可離線的代理商系統。

(七) V 模型公司：自動的用戶資訊 downloading。

最近一個高爭議的案子是亞馬遜控告 Amazon.com 侵犯它的專利—「按入技術」，即僅僅允許用戶列表和裝載資訊，然後輸入這個相同的資訊到另一個地方。聯邦法官針對這種情況下了初步命令 Barnes and noble.com 使用這樣的技術。其他違犯專利的情況也曾發生在 AT&T 公司、雅虎公司、微軟公司和 Priceline.COM 等知名大公司。

四、隱私權的風險（privacy risks）

隱私權是現今的熱門話題。無論組織在網路上最小限度是否存在，它需要意識到與線上秘密聯繫的危險。如果組織不提出這些危險，責任可能變成組織的了。

（一）隱私權的法律（general law of privacy）

常見觸犯隱私權的例子有四：

1. 秘密侵略是侵權行為又叫不合理入侵
2. 個人的名字與商業優勢同等不得侵犯
3. 出版關於私人秘密的出版物
4. 把他人隱私放在非法光碟裡的出版物（與誹謗類似）

觸犯隱私權是指未經許可即使用或是入侵他人的隱私，甚至惡意的出版，不計後果，任意散佈訊息。值得一提的是隱私權僅僅涉及個人，公司或其他商業組織並沒有秘密的權利 (但他們有類似權利，如商標和商業秘密)。誹謗亦是一種侵犯隱私的行為，一旦有下列情形即可能構成誹謗罪：

1. 言語攻詰
2. 涉及他人隱私
3. 在出版物中刊登誹謗他人的文字
4. 以不當言語、批評破壞他人的名譽
5. 誹謗語言的錯誤
6. 被告的部分錯誤

隱私權是美國賦予個人保守秘密的權利。1986 年 ECPA 通信隱私權保護法案對指狀通信（包括細胞電話，電子郵件，電腦傳輸，和聲音和顯示的 pagers）擴展聯邦的竊聽行為。ECPA 禁止所有人、商業、和政府未經許可竊聽、探搜或干擾電腦系統儲存或傳輸中的資訊。但如果在操作員和用戶之間的用戶秘密上事先聲明(e.g 公司的電子郵件策略)，當公司想存儲系統方面的用戶資訊時，便不算違反隱私權法。同樣地，老闆有權利存取雇員的電子郵件。

（二）電子商務與隱私權（privacy and E-commerce）

隱私權可能是使一些人不敢使用網路或者參與電子商務的主要原因。沒有經過本人的授權，即收集或散佈個人資料，對商業、政府、個人和隱私權本身都是一件很嚴重的事，因此隱私權對電子商務而言是不容忽視的。

五、匿名書記（anonymity/cookies）

匿名在電子商務世界幾乎不可能。cookies 是轉移用戶電腦的代碼，網路網址操作員利用 cookies 便可知用戶在哪裡和做什麼。電子秘密資訊中心通常沒有經過用戶的同意，即允許網路網址記錄用戶的 comings 和 goings，是值得一提的嚴重秘密事件。

六、大量廣告郵件（spamming）

Spamming 是未經請求的廣告透過電子郵件或其他方式送給群眾。大量的廣告郵件會使電子郵件系統變速甚至被迫關閉，造成嚴重的破壞。Spamming 的產生大多數涉及 ISPs，應用導向語言、線上資料庫服務，可以防止用戶收到大量的電子郵件。法院認為被告郵寄假電子郵件給用戶迫使其接受，已經違反了「網路規定」的原則。

七、加密（encryption）

合法的加解密涉及編密碼技術及其軟體的輸出。商業界一直積極發展編密碼策略，他們認為這樣將可控制全球。美國於 1952 年限制了編密碼技術，因為技術一旦被誤用，將對軍事和工業產生不良影響。柯林頓時曾提出放鬆編密碼約束的新編密碼規則，允許任何用戶輸出任何零售的編密碼產品，再由輸出管理局決定哪個作為零售產品，但新規則並沒有獲得政府的許可。輸出編密碼技術在外國有一些限制，如輸出到古巴、伊朗、伊拉克、利比亞、北方朝鮮、蘇丹和敘利亞等國仍然有禁令，而編密碼軟體的輸出地仍然是很容易改變的地區。

八、探測郵件（E-discovery）

E-discovery 提供合法探測電子郵件和其他的電子通信的管道。在硬體、軟碟、卡帶、備用支援磁盤，和其他電子裝置的儲存上的文件和資訊都容易被發現, 例如細胞電話、資訊錄音裝置, 和網路間的伺服器文件。甚至在電子郵件刪除了以後，還能夠重新取得。多數公司使用備用支援卡帶儲存一年內的電子郵件資訊。在某些情況下，這些卡帶在利用以前，電子郵件能夠提供有價值資訊。但是，收集電子郵件不僅必須擔憂電子郵件的內容，且分類電子郵件所需費用可能很昂貴。

九、廣告和出版的風險（advertisement and publishing risks）

網頁的環境為廣告和出版風險的溫床，以電子媒介來誹謗

人、機構或公司的例子很多，主要的風險有廣告和娛樂等，尤其是創意和編輯方面。下列幾個風險和內容相關：誹謗、隱私、不實廣告、詭計、侵略或智慧型的偷竊行為，都會觸發法律責任引起訴訟。透過電子媒介和印刷品的言論自由與口頭上的發布有極大的差別，尤其是發布的寬廣度更大，在這個方面，電子公佈更類似報紙的風險。佈告欄是個人受損公佈最基本來源，受損可能會被雇員、交易夥伴，或者局外人發布，但是廣告設計上的錯誤，例如使用者相似，誤用電子郵件、聊天室也會招致個人或者組織的損害，而無限的群眾更擴大消息流傳的潛在地。網路改變了傳統的銷售方式，多數公司使用廣告代辦處創造或者遮蔽銷售的材料，透過網路直接聯絡買方，成為真實市場的廣告者。

十、消費者保護與公平交易風險（consumer protection and unfair trade practices risks）

網路上的惡性競爭或欺騙行為常造成使用者額外的損失或責任。廣告的公司，向搜查引擎供應者購買關鍵字，當這些使用者在搜查引擎鍵入關鍵字以搜尋特定公司或產品時，即會連結某些貿易行為，而在網路上看到化粧品公司或其他廣告。美國安全和交流委員會，已經在它的網路加強搜尋的能力，以遏止上述現象。

十一、專業風險(professional risks)

專業風險常發生在有能力的人身上，例如網路設計者、ISPs、軟體開發者、安全系統開發者和顧問等。常見的專業風險包括架構、設計、編碼的錯誤、不適當軟體、安全認證的失敗、設備或者軟體的規格錯誤和編輯疏忽。

網際網路的專業包括網站的設計；電子郵件系統、線上查詢、聊天室和佈告欄的操作；編密碼技術的發展和專職的服務。例如超連結設計上有瑕疵時，可能產生原先不存在的商業關係。如果在安裝上列專業設備時，專家不回顧設計，將可能導致某些網路責任。此外，設計上的瑕疵可能方便他人或駭客閱讀電子郵件，引起專業風險。不久前，一些電子郵件的系統中因為專業設計上

的瑕疵，引發抱怨的聲音，尤其那些免費上網的人。

十二、服務否定風險(service denial risks)

服務否定風險，是所謂 E-commerce 的第三者風險，除了合法的責任以外，服務否定可能會有深遠的影響。服務否定責任不應該與「服務的分發否定」搞混，這樣將會混淆是由哪一個電腦系統解決，造成混淆服務否定與服務中斷。

第三者不能連結服務公司的網路網址，或要求服務時遭到拒絕時，都屬於這類第三者責任險。例如，駭客攻擊某網路時，管理者將網站關閉，不能連結的顧客或商業夥伴，可能就遭受損失而提出訴訟。如果有顧客或者夥伴聲明拒絕連結公司的快速通路，也會產生損失。駭客的攻擊並非都能成功，但是卻能使連結的速度慢下來，影響公司的信用、名譽、儲備價格和銷售份額，而必須轉移重要的資源，以解決服務否定的危機。

十三、未來第三者風險(future third-party risks)

未來第三者風險是現今電子商務的重要風險之一。網路網址尤其需要從事電子商務的公司從旁管理。做廣告必須先由網路網址操作員鎖住 domain name，秘密是電子商務另一個主要的風險，秘密和個人資料的盜取和外流是電子商務公司的嚴重風險。在這個章節中所討論到的風險，僅是風險當中冰山一角，當電子商務發展日益蓬勃時，其他風險肯定會增多。

第四節 風險管理方法

適當的災禍處理和保險能降低電子商務的風險。防止網路聯結、電子郵件、秘密分享，或策略等非技術的風險，除了正確的策略、程式外，還必須有專門的硬體設備或資料處理的安全技術。

電子商務公司的風險管理人員在該公司發展程式時，應該瀏覽他們的出版物和網路網址，列出電子商務、電腦以及任何可以顯示出該公司產品、網路服務和軟體的路徑，再和專業的機構討論公司的合法

責任，並與保險顧問商談問題的徵結。

圖 2- 1 職責管控金字塔

資料來源：參考書籍 R1（六）

一、識別和評價

電子商務的風險管理應先判斷損失的來源，評估商業策略、過程、契約及傳播系統、通信、途徑、資料存儲或廣告內容的安全性，並考慮財政、商業和個人的資料，方便稽查損失的來源。評估電子商務風險，應針對重要的策略做改善及入侵測驗，檢查程式和系統是否易受非許可雇員、服務和設備供應商、駭客盜取。

二、安全測試網際網路

架構確定和獨立系統地區的分析不會被信任的組織控制，途徑的識別和估價控制：特權證明書、草案、鑑別草案、編密碼、應用的防護、惡意代碼防禦，或者封包過濾；系統權力登記的回顧和途徑允許的自動回復的程式，可以用來分析使系統破壞或者中斷所造成的影響。

三、稽查形跡的估價

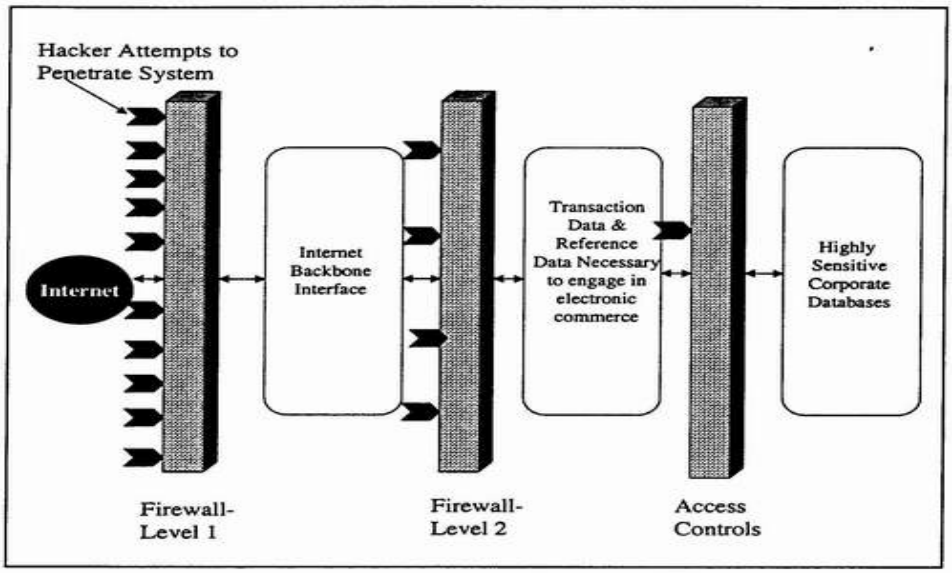
恢復網路中斷的方法，包括管理公共的網路和能力的回顧；商業連續性檢查可以決定系統元素的失敗將如何影響其他元素，

包括供應商和顧客的系統；用戶和雇員用智力去違反實際策略的估價；公司用來回顧發行的策略，包括網路網址、做廣告、資料保持和危機的管理，以上這些項目雖然對電子商務好像無關。不過由熟練稽查者對整個過程的獨立估價，將有助風險的識別。

四、電子商務風險管理技術辦法

使用備用支援系統是控制電子商務的方法。雙重系統資料備份改進了網路間的工業標準，在從事電子商務的電腦間，鑑別通信的途徑(包括命令、計畫同意，或者硬體、軟體、資料庫、文件、網路、系統、應用等等)。使用防火牆即為一種鑑別和權力批准途徑的程式，圖 2-3 為防火牆的防護階層。

圖 2- 2 防火牆防護階層



資料來源：參考書籍 R1（六）

能夠把這些技術辦法分成下面的範疇：

（一）資料和資訊的安全

（二）備用支援系統和冗餘

（三）備用支援系統的廣泛使用

通常損失預防測量，就是備用支援系統的廣泛使用。這些是指完全都靠備用支援文件和備用支援的設備。二者可能在網路和有效的持續操作時都十分重要。這個結合可評論系統是否能夠持續營運。

五、資料和資訊安全

安全是指可能在公司外面或者從其裡面破壞。駭客可能獲得重要公司文件的通路，或者他們可能釋放病毒破壞或者改變文件。根據 KarenL.Casser 指出：駭客對公司文件的偷竊行為相當於十億個生意，當公司在網上從遠端登入他的網路時，能夠用各種技術對資料和資訊的傳輸中添加安全。

六、指紋辨識

舉例而言，就是讓使用者附加獨一無二的簽名，對是否已經改變了文件做一個辨明。能夠由回顧電腦系統產生的連結來追蹤一些電腦犯罪。多數的網路連接的電腦都會自動地創造一些線索，來尋找以前連接過的痕跡。

七、密碼（passwords）

透過口令和編密碼技術，在網路上提供了資料和資訊的安全。外部入侵，是透過公司的本身，如很多公司意識到他們易受未經許可系統入口去入侵自己的電腦。根據公司所請的駭客，在他們自己的安全系統中查詢觀察，發現很多網站被入侵都是因為口令的誤用。公司口令太簡單或太明顯，就會被外部任何人入侵；有時系統管理人離開時，口令沒有適時調整，亦容易被入侵。

八、通訊協定（protocols）

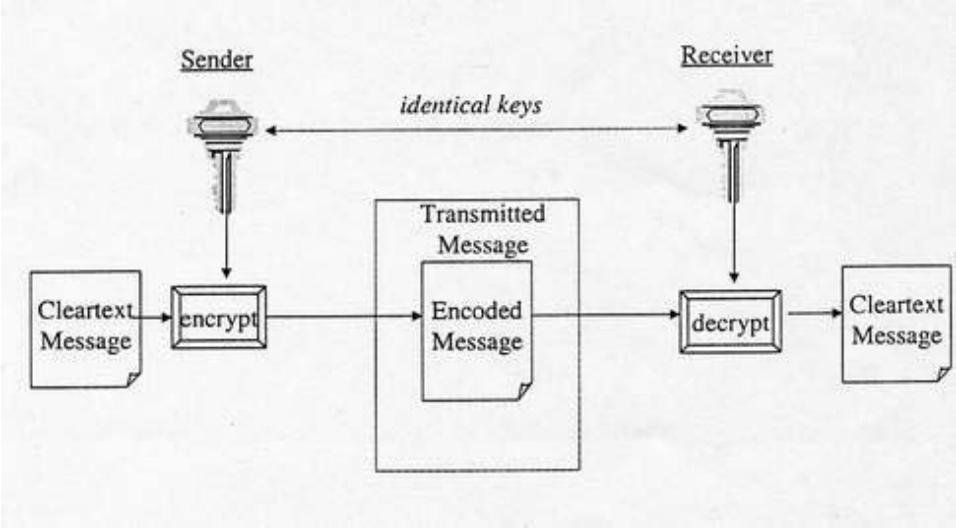
程式在設計和保持安全系統時也有其重要性。由發送器和接收器之間的程式上提供了安全，尤其當涉及國家安全或者財政的會議記錄。有一個系統叫作 SSL，利用公開鑰匙密碼技術在網路

上保護交易的安全, 以確保電子處理事務。這系統需要三個方向：個人、買賣的公司和財政的機構。系統可在網路上保護支付行為, 以證明書確認持證者和商人具有相同的負擔，並以密碼的形式, 避免在網上公開揭露交易的數字。

九、加密

圖 2-4 為加解密的示意圖。資料加解密碼軟體會使原先的資料混亂，使其不易閱讀。此加密技術是一種非指數的運算，經過編密碼軟體之後，使資料變為亂碼，然後再利用破譯鑰匙，將原資料解出。以下兩個技術為設計編密碼的方法：

圖 2-4 加解密示意圖



資料來源：參考書籍 R1（六）

（一）個人金鑰：發送器和接收器使用相同的編密碼鑰匙或者演算法，如：DES。

（二）公開金鑰：這個系統使用一個私鑰，把資訊譯成密碼，再用公開鑰匙去解開，如：RSA。

傳送訊息是用公鑰做加密來傳，有私鑰的人才能解開。而世界各地都有其一套的系統在做這一方面的事，美國目前限制軍事上或是在國際交通的保護罩下輸出編密碼技術。歐洲也限制編密碼技術，在歐洲委員會的雙重使用商品規則下輸出。

十、電子郵件收發管理辦法

公司應該為網路和電子郵件的使用做適當的控制，實施雇員使用電腦的固定稽查；安裝對雇員使用網路的某種控制的軟體；研發網路路徑和電子郵件控制。發展網路路徑和電子郵件的策略將有助電子商務的控管，把通信系統作適當的等級區別，並且讓雇員在公司的通知命令上簽名，讓他們承認已收到此通知，這通知內容應該包含如下：

（一）誰有上公司網站系統，及收發公司電子郵件?

（二）在什麼時候雇員可以存取網路?

（三）如何創造和分發口令?

（四）系統的目的是什麼?

（五）對於用戶的秘密期望是什麼?

（六）違反的處罰是什麼?

（七）如何保留電子文件?為期多久?

（八）什麼時候從系統刪除文件?

（九）使用什麼類型編譯密碼方法?

（十）如何通知雇員公司策略？或者策略違犯的懲處?

第三章 電子商務產業領域風險現況

第一節 電子商務六大產業領域

在現實的世界裡，商務交易行為需要一套複雜的基礎架構來支撐。當然，電子商務和雜貨店一樣需要另外一套龐大又複雜的基礎架構來支援，這個基礎架構由成千上百萬個不同的環節組合而成，建構這些環節並將之串連在一起就是電子商務六大產業，如圖 3-1 所示：

圖 3- 1 電子商務產業的結構

<table>
<tr><td colspan="5">商務內容</td></tr>
<tr><td colspan="2">安全</td><td>電子付款</td><td>金融服務軟體</td><td>商用軟體</td></tr>
<tr><td rowspan="3">基
礎</td><td colspan="4">網際網路軟體工具和語言（爪哇〔Java〕、Active X、“ Push ”）</td></tr>
<tr><td colspan="4">網際網路基礎架構（標準、通訊協定、NAPs、MAEs、ISPs）</td></tr>
<tr><td colspan="4">電信基礎架構（電話線、數據專線、光纖電纜、COs）</td></tr>
</table>

資料來源：參考書籍 R3（一）

一、基礎產業：含三個次領域

（一）電信基礎架構：

構成電話系統的電話線（plain old telephone lines，POTs）、數據專線（leased lines）以及光纖電纜，現在更包括無線、有線和衛星的運用。這個基礎架構提供基本的電子連結，讓網際網路以及電子商務得以落實。

（二）網際網路基礎架構：

網際網路的開放標準（open standards）、通訊協定（protocols）和網路互接點（network interconnection points）的設立，讓網際網路無遠弗屆、吸引全球上網。

（三）網際網路軟體和工具：

用來開發網際網路軟體的基礎軟體語言、科技和開發工具。電子商務產業運用這些工具來創造電子商務專用的應用程式和服務。

二、安全產業：

提供讓企業和消費者安心使用電腦網路的軟體、硬體和服務。這個領域銷售的產品和服務有防火牆、加密工具應用套件（encryption tool kits)、付款安全軟體（payment security software）和數位認證（digital certificates)。

三、電子付款產業：

為企業、消費者和金融機構開創、處理和分析各種型式的電子付款。這個領域銷售的產品和服務有付款處理（payment processing)、電子轉帳繳費／帳單提示（electronic bill payment／presentment）和電子現金（electronic cash)。

四、金融服務軟體產業：

開發讓企業和消費者可以利用網際網路連接、管理及分析金融帳戶的軟體。這個領域銷售的產品和服務有網路銀行軟體（Internet banking software)、線上交易軟體（on-line trading software）和理財軟體（financial management software)。

五、商用軟體產業：

提供企業界所需的軟體和服務，將企業內部付款、匯款、庫存和訂貨系統網際網路連結。這個領域銷售的產品和服務有電子目錄軟體（electronic catalog software）和電子資料交換（electronic data interchange，EDI）軟體／服務。

六、商務內容產業：

這個領域的組成份子是真正透過網際網路從事零售或批發的公司。這個領域的商家和企業運用前各項領域所有的產品和服

務，提供消費者和企業可以透過網際網路進行價值轉移的服務。這個領域銷售的產品和服務有書籍、光碟、酒類、工業用品和橡膠樹脂等。

表 3- 1 六大電子商務產業的定義

產業	定義	次領域範圍	代表公司
基礎	提供基本的電子連結，開放通訊協定及軟體開發工具。	. 電信基礎架構 . 網際網路基礎架構 . 網際網路軟體和工具	. Hinet . Seednet . Tanet
安全	電腦網路的保全。網路上採購、付款各方的認證與鑑定。	. 網路安全集團 . 加密工具廠商 . 認證機構	. Security Dynamics . Verisign . Checkpoint
電子付款	電子付款的開創、傳送、處理與分析。	. 信用卡付款處理廠商 . 轉帳繳費與帳單提示 . 付款支援廠商	. First Data . Checkfree . Gemplus
金融服務軟體	讓消費者和企業可以與其金融帳戶及相關的資料取得線上連結的軟體與服務。	. 消費者軟體 . 企業軟體 . 中介軟體	. Intuit . EC Partners . Integrion
商用軟體	讓企業將內部的付款、匯款、訂貨和庫存系統與網際網路連結的軟體和服務。	. 開放式商務交換（OCE） . 電子資料交換（EDI）軟體和服務 . 直接資料互動（direct data interaction，DDI）	. Sterling Commerce . Open Market . Crossroute
商務內容	主要的組成份子是真正透過網際網路從事零售或批發的公司。	. 購物 . 金融服務 . 工業採購	. Amazon.com . E*Trade . Onsale

資料來源：參考書籍 R3（一）

第二節 基礎產業安全機制的風險

一、網際網路成長率趨緩

電子商務產業的預估價值高度依賴網際網路的持續成長和發展，網際網路的成長若出現不符預期的遲緩現象，會對整個產業的價值產生深遠的影響。儘管如此，第一資料公司和 First USA 等根基穩定的付款處理公司可能只受到輕微的波及，能夠安然度過風暴，因為現階段它們尚未廣泛利用網際網路。

二、安全「出現瑕疵」

本書的下二節將探討安全的問題，以破除人們以為安全的結論問題深深影響到電子商務成功與否的迷信。但許多可能發生的安全「事件」會讓電子商務產業突然降溫，其中包括：

（一）知名的電子商務網站遭人入侵，業務營運受到破壞。

（二）有人透過網際網路入侵大型銀行或經紀商，盜領顧客的大筆資金。

（三）輕鬆「破解」加密運算的方法研發成功。

儘管我們認為基礎科技十分健全，但未來數年，投資人會因為對系統短暫失去信心而歷經若干次的安全「恐慌」。

三、提防「大象」

光是微軟的市值就幾近整個電子商務產業的 4 倍，IBM 和甲骨文等大公司也非等閒之輩。這些公司就像大象一樣：愛來就來、為所欲為，不識相的就被一腳踩扁。電子商務產業的投資人要留心大象的動向，避免投資任何擋他們道的公司。

四、最後一個「小小的」提示

我們必須指出，電子商務產業股票和大部分高成長股票一樣，當利空消息出現時，電子商務產業股票的股價呈現的不是修正，而是無量下跌的局面，一天之內跌掉一半時有所聞。投資電子商務產業的風險很高，在這尚未成熟的初期階段，風險更是高

得驚人。不習慣這種高風險的投資人短期之內最好不要輕易涉足。

五、安全機制的風險

不幸的是，沒有一個安全措施是十全十美的，儘管有優良的科技助陣，電子商務還是有一些潛在的安全風險，至少就目前而言，這些風險是無人可以預防的，包括：

（一）個人密鑰可能遺失：

或許這不該被稱為風險，因為這種事情一定會發生，就像人們會弄丟車鑰匙一樣。每當有人遺失個人密鑰，別人就有機會利用它來做一些不法的行為，但由於電子商務安全措施目前是萬眾矚目，所以只要發生一宗知名的竊案，電子商務被人接受的時程可能就會延後許多。

（二）重要認證機構的密鑰可能遭「破解」：

儘管相關人士已經嚴加防範，但政府、威士卡或萬事達卡等重要認證機構的密鑰遭人竊取仍有可能發生。這種事雖然稱不上是災難，但短期之內若發生這種事，很多人對透過網際網路進行交易就會感到不安，進而阻礙了電子商務的成長。

（三）公共密鑰科技可能遭「破解」：

若說這是一場災難絕對不會言過其實。數學理論極可能出現重大突破，讓公共密鑰科技的破解易如反掌。所幸在過去二十年當中，許多世界頂尖的人才，花費數十億美元的經費想要破解公共密鑰科技，結果卻沒有大大進展。不過，數學領域若有重大的發現，整個公共密鑰科技一夜失守的可能性還是有的。就目前而言，這樣的發現影響不大。但十年之後，可能會是電子商務產業的 「黑色星期一」(Black Monday，編注:指 1987 年 10 月 19 日星期一紐約股市大崩盤)。由於可以改用其他「未被破解」的公共

密鑰運算法，所以不會落得失去一切。即使在最惡劣的情況下，也可以回頭再度採用對稱式密鑰科技，但大多數公司並不喜歡這樣的交易方式。

六、結論

即使所有的人都使出渾身解數，電子商務產業也不可能百分之百安全。然而，當所有的安全機制一一就緒，電子商務環境的安全性很可能超越現有的商務模式。例如，現行的書面式證件和親筆簽名讓每年的信用卡盜刷案超過 10 億美元，支票詐欺案也超過 8 億美元。本章所介紹的科技大幅提高支票詐欺案、信用卡竊案和偽造案的難度。我們不敢說這些新的安全科技可以杜絕犯罪，卻可以降低犯罪率，同時還能實現隱密、自發、互信的電子商務夢想。

鑒於五年後網際網路的規模可能為目前的 3 倍或 4 倍，科技成本持續下降，功能卻顯著提升，預期電子商務產業在未來幾年會出現爆炸性的成長。事實上，電子商務產業超高的價值就顯示出很多投資人都有同樣的看法。電子商務產業的挑戰在於不使自己陷入主要的安全危機，也不要無端惹惱「大象」；投資人的挑戰則在於找出致力於在致勝關鍵上求發展的公司，而這些致勝關鍵會幫助企業獲致長期的成長和盈餘。

第三節 安全領域風險

隨著整個產業繼續演進，安全領域會有四大風險：

一、來自網路和作業系統公司的競爭

大型的網路和作業系統公司是安全科技發展的既得利益者。目前，這些公司大都選擇和現有的安全領域公司合夥，以擴充它們的安全產品。不過，這些大公司一旦決定自行發展「內建」解決方案，可能就會嚴重影響到安全領域的長期成長，甚至威脅到其獨立地位。值得注意的是，只要任何一家安全領域的公司被

大型公司購併，就有可能損及其他公司的價值。這些大型公司具有龐大的現金流量，且習慣透過購併追求成長，這種情況確實有可能發生。安全領域所面對的風險或許就是地位太過重要，以至於成為各方覬覦的目標。

二、法律方面的風險

一般預期美國政府會持續放鬆其出口禁令，且可能在 21 世紀來臨之前予以廢除，若政府發表與此預期相反的言論，將對這個市場造成嚴重的打擊。此外，政府隨時皆可要求企業嚴守法律上的規定。這會影響企業的營運開銷和市場彈性。政府也尚未擬定與認證機構市場相關的計畫。政府可能禁止私人公司從事認證機構的業務（可能因為認證機構需要較長的密鑰），果真如此，對安全領域絕對會產生負面的影響。

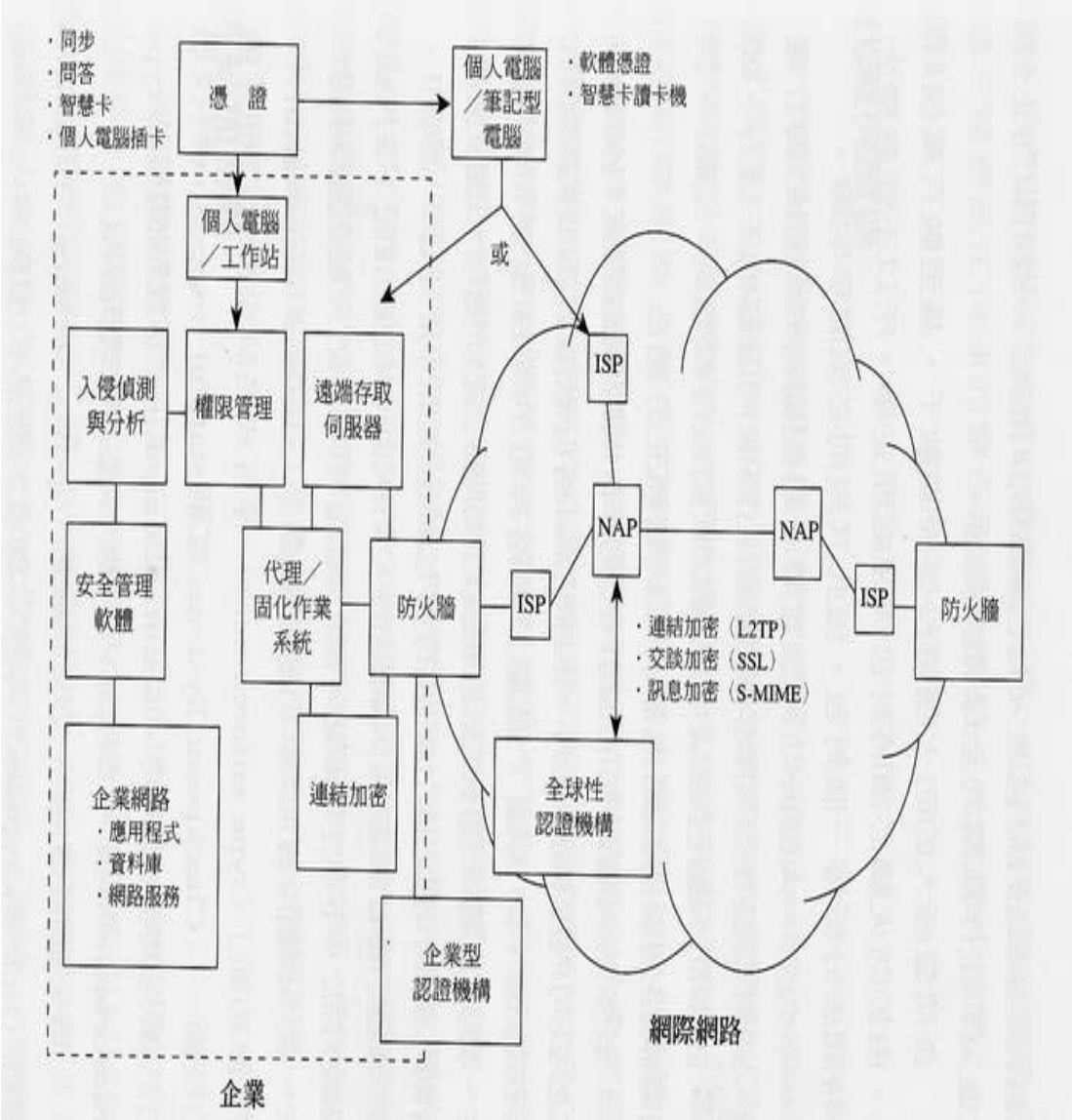
三、安全電子交易標準（SET）的普及

前面提過，市場中有很多人預期 SET 會獲得普遍接受。很多安全領域公司只針對 SET 市場來製造商品。而市場看好其前景的心態也都反映在它們的股價上。因此，SET 的普度和接受若出現任何的問題，可能會對整體安全領域產生負面影響。

四、結論

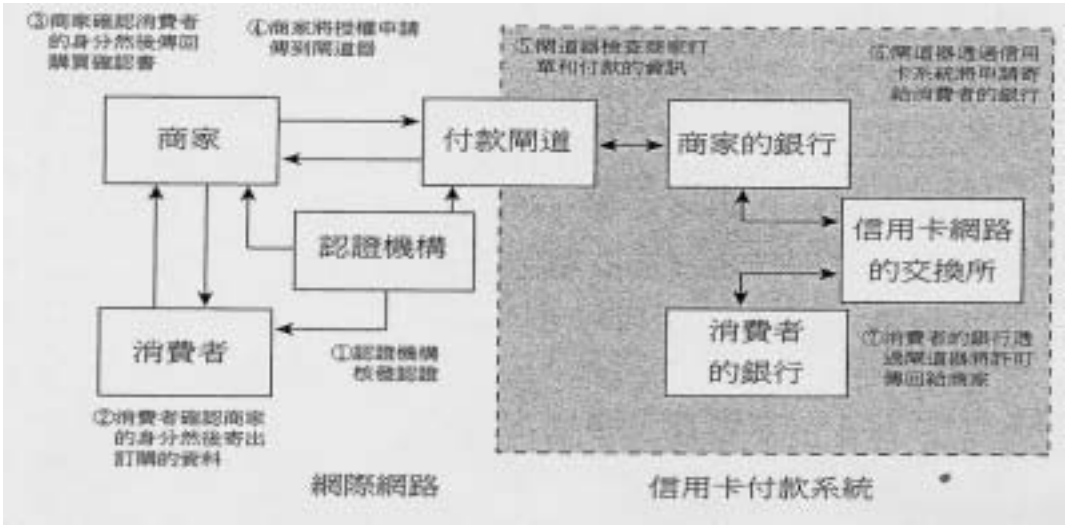
過去數年來，數個強勁的驅動力造就了安全領域驚人的成長且受到萬眾矚目。未來幾年，市場的基本驅動力應該還是相當的強勁。安全領域最大的挑戰是從分散的產品和服務，轉變成一套以業務為重心的解決方案。當安全領域的公司致力於從科枝和工程轉移到顧客和市場之際，也就是轉型的時候。這些公司最大的挑戰在於找出適當的定位，以便於和大型的網路設備以及作業系統廠商的安全產品達到互補與共存。圖 3-2 至圖 3-4 為相關安全領域的架構圖。

圖 3- 2 安全領域現階段的架構



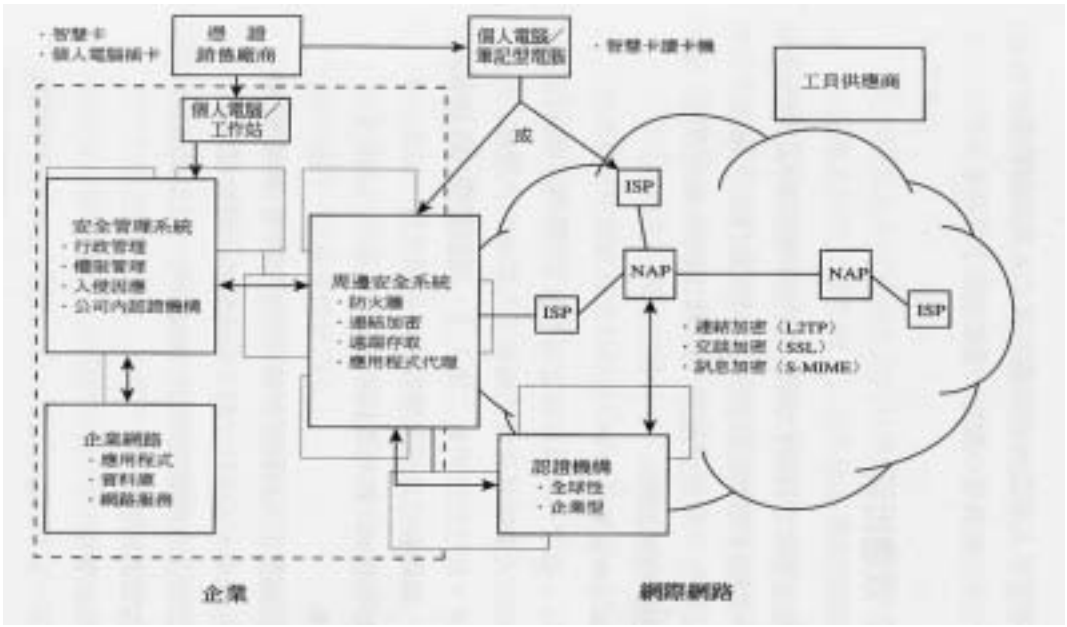
資料來源：參考書籍 R3（一）

圖 3- 3 SET 付款授權流程圖



資料來源：參考書籍 R3（一）

圖 3- 4 安全領域最後可能出現的局面



資料來源：參考書籍 R3（一）

第四節 電子付款領域風險

儘管各方都認為這個領域的基礎相當穩固，但仍然有一些風險會對這個領域造成負面的影響：

一、「反彈」

金融服務業漸漸出現嚴重的「懊惱症」。很多金融服務業的主管眼電子付款公司高達 20%至 25%的成長率及傲人的本益比，悔不當初的公開表示已讓好機會從自己的手中「溜過」。金融服務公司這樣的感受越深，對非金融機構產生反彈的風險就越高。這種「反彈」會讓委外處理的數量減少，甚至造成銀行重整其處理企業聯合的局面，二者都會讓第三方電子付款處理公司成長減緩。

二、合併

金融服務業的合併以穩定的速度持續進行，合併得越厲害，電子付 公司潛在顧客人數就會漸漸減少。對於營收主要來自少數幾個顧客（而這些顧客又可能是被收購的對象）的公司應該特別小心；對於產品主要銷售給商家的公司，這個問題就不是那麼迫切。

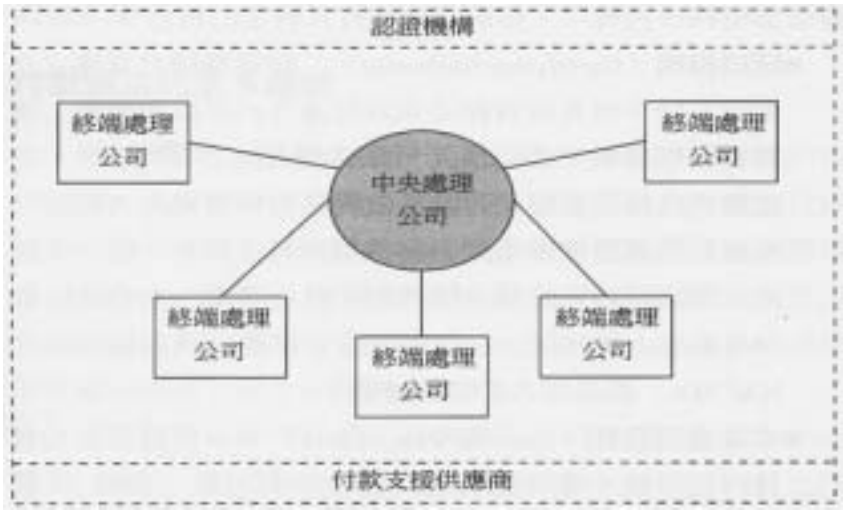
三、定價

公司經過一番努力創造出具有附加價值的產品和服務，但它們卻無 忽略一個事實, 那就是身為公司核心業務的付款處理終究還是一項商品。目前的價格競爭相當激烈，但隨著公司的規模日益增大，它們會用越來越強的規模經濟價格承受更大的壓力。價格大幅下挫會對獲利產生莫大的影響，尤其是對中型的公司。我們預期階段性的價格戰和恐懼會損及產業的價值，但這也是收購定位正確公司的大好時機。

電子付款領域在電子商務產業中舉足輕重。早在網際網路和全球資訊網深入家庭之前，這個領域就已經在處理電子付款了，而且，不管電子商務產業的其他領域發展如何，這個領域還是會繼續扮演單調卻重要的角色。儘管這個領域在過去數年當中成長快速，但不管是國

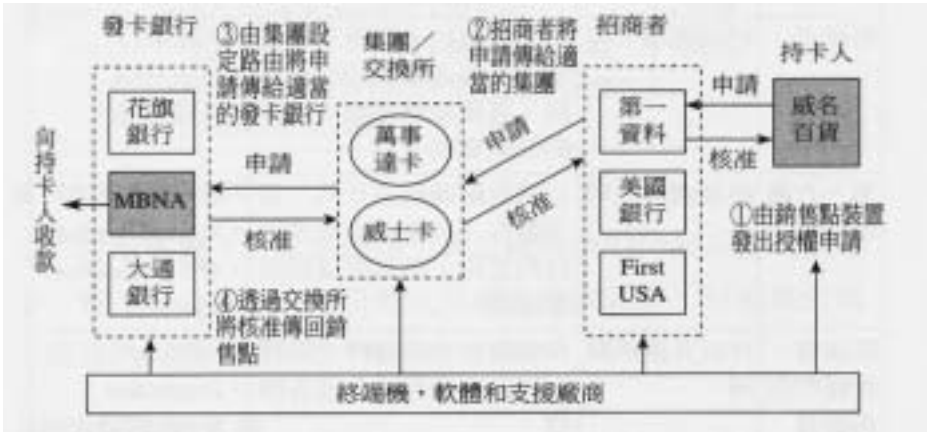
內或是國外市場，似乎都還蘊藏了許多機會，所以至少五年之內都能持續這樣的高成長。電子付款公司的重要課題在於找出正確的定位，不但要在合併風氣下求生存，還要讓事業蒸蒸日上，積極將業務拓展到電子付款的各個層面、具備向海外發展的策略、努力求進步又不失技巧的大公司，最有可能在這個深具挑戰性的環境中生存下來。圖 3-5 至圖 3-10 為相關電子付款領域的架構圖。

圖 3- 5 付款系統結構的共通點



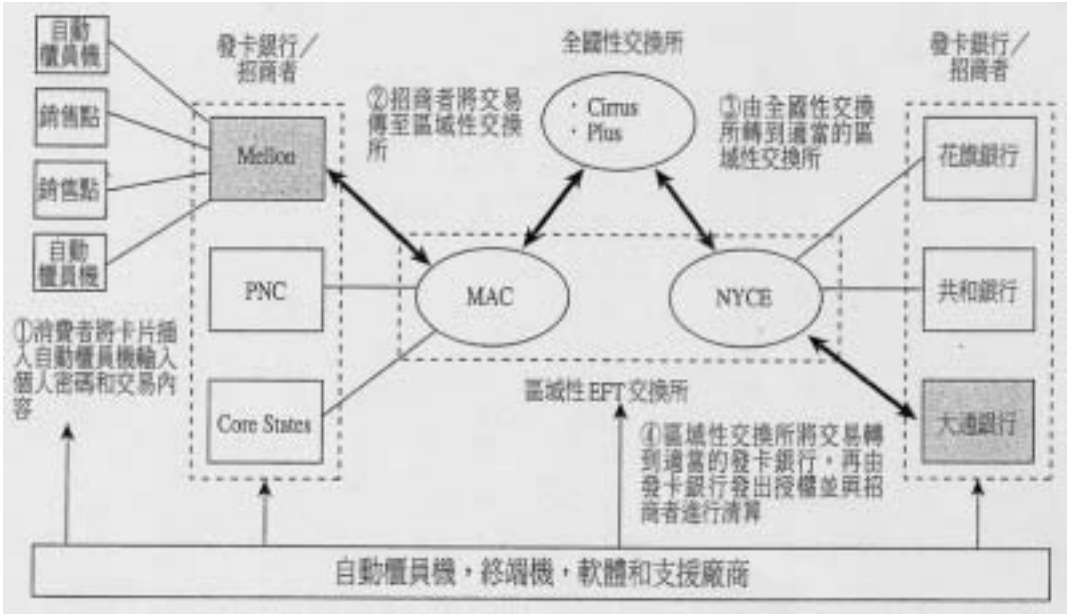
資料來源：參考書籍 R3（一）

圖 3- 6 信用卡交易流程



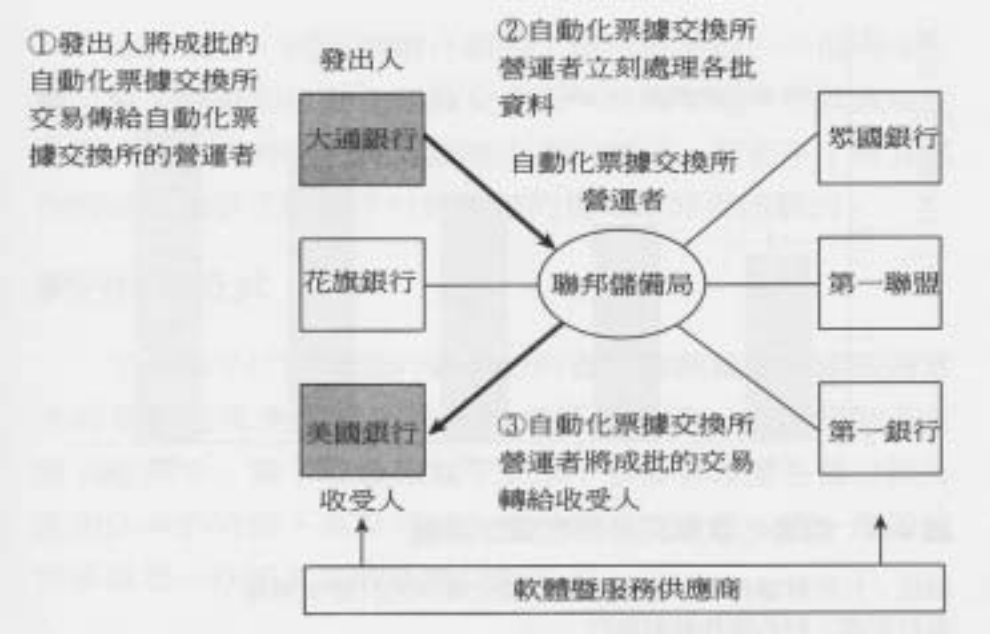
資料來源：參考書籍 R3（一）

圖 3- 7 電子資金轉帳交易圖



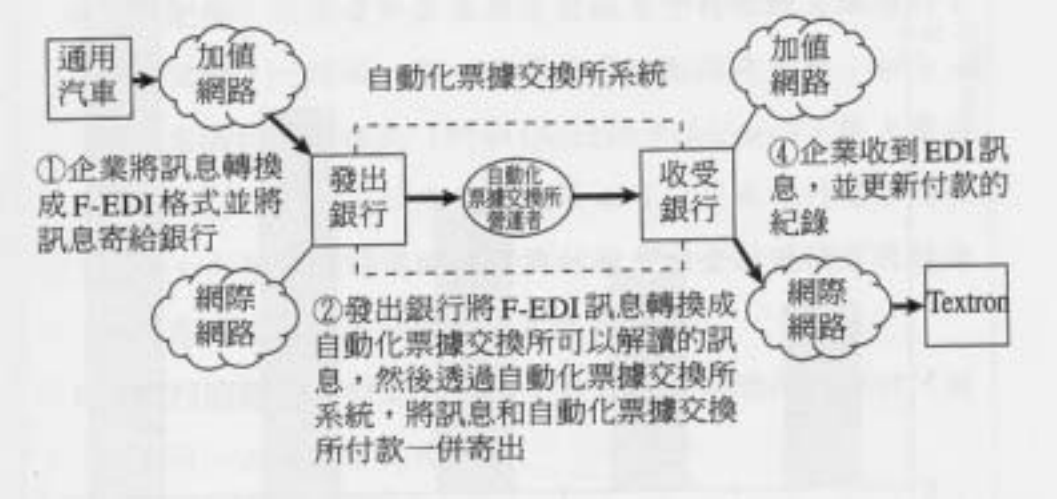
資料來源：參考書籍 R3（一）

圖 3- 8 自動化票據交換所交易圖



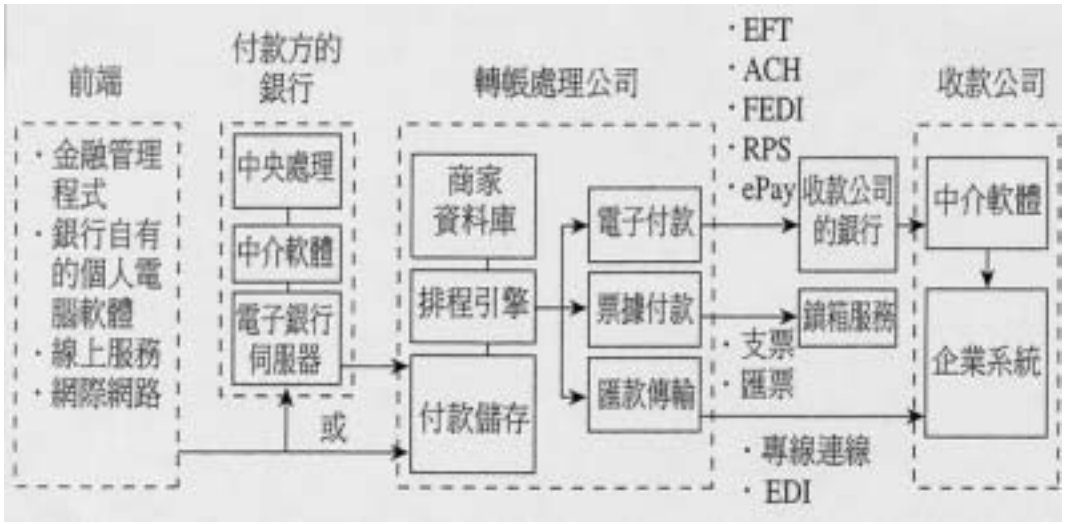
資料來源：參考書籍 R3（一）

圖 3- 9 F-EDI 交易圖



資料來源：參考書籍 R3（一）

圖 3- 10 電子轉帳繳費交易流程圖



資料來源：參考書籍 R3（一）

第五節 金融軟體領域

在金融機構、微軟和 IBM 之間互相角力的同時，投資金融軟體領域自然要冒一些風險：

一、線上銀行/線上經紀的接納程度趨緩

預期五年內線上銀行和線上經濟會成長 5 倍到 7 倍。若成長率不如預期，這個領域會出現相對的跌幅。個人電腦 / 網際網路普及率趨緩會是這個趨勢的明顯指標。

二、安全漏洞

對進行線上銀行活動的消費者和企業而言，安全是非常重要的考量。金融機構的線上業務若出現廣為人知的安全漏洞，消費者接受線上銀行服務的意願會普遍下降，進而促使許多金融機構重新檢討當前的業務。由於網際網路上金融機構所採取的安全防護參差不齊，形成投資金融軟體領域的一大風險。

三、Integrion

Integrion 身為北美 18 家大銀行的「優先考慮供應商」，讓它對市場產生很大的影響力。lntegrion 若決定進軍任何次領域或新興的領域，都會嚴重影響到金融軟體領域其他公司的投資前景。此外，lntegrion 若決定支持某家公司的產品或服務，也會對該公司競爭對手的價值造成負面的影響。

四、價格策略

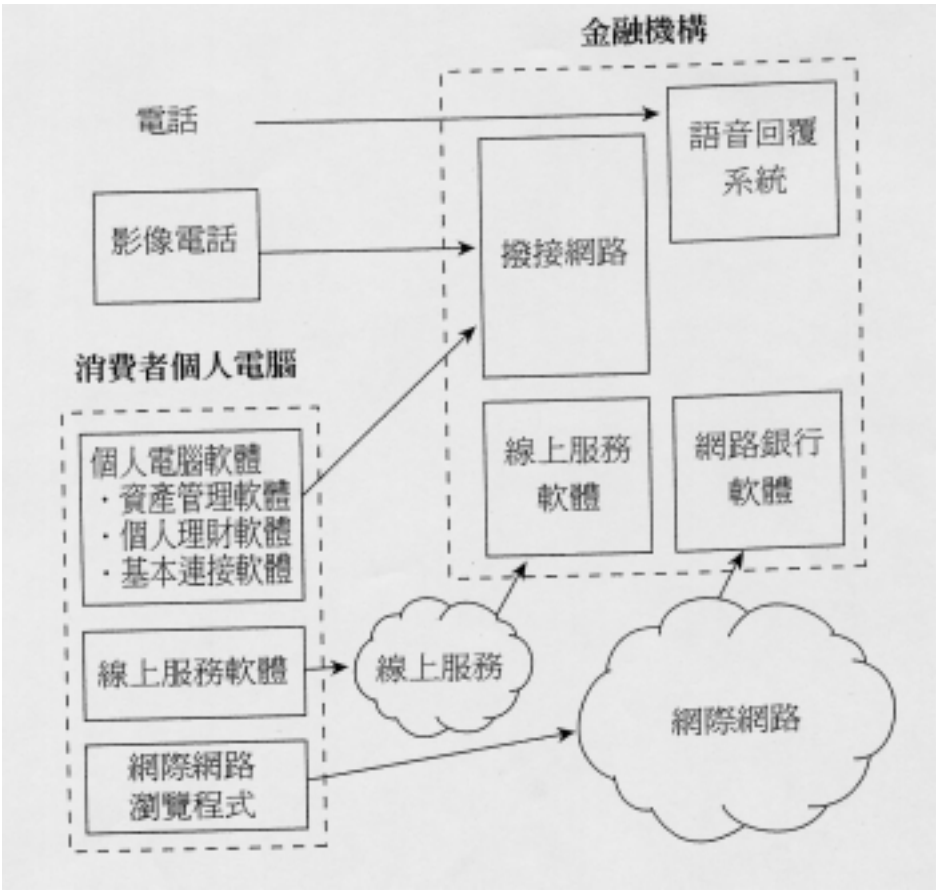
由於微軟免費提供前端軟體給銀行以爭取網際網路伺服器、瀏覽程式和開放金融交換訊息標準的業務，目前整個領域的價格呈現不穩定的狀態。所以，和微軟正面抗衡的公司會面臨價格競爭激烈的環境。

五、結論

金融軟體領域還是一個新興市場，由於主要的驅動力在未來五年預計有 5 倍到 7 倍的成長，所以這個市場顯然也有大幅的成

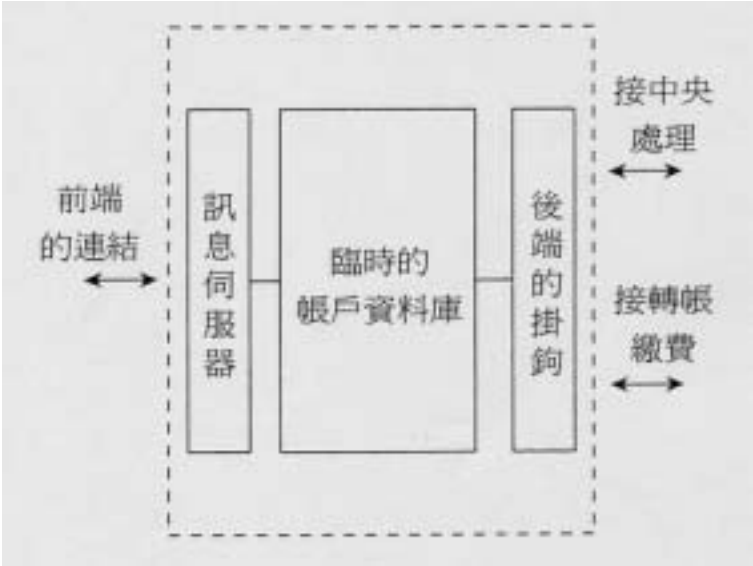
長空間。隨著市場成長，這個領域的重要性也跟著提高，因為市場的主流會從只提供連接服務，轉變為提供整合等具有附加價值的產品，將金融機構與電子商務產業連結，拉近與顧客的距離。這個領域的成功關鍵在於集中心力提供應用程式和服務，讓金融機構在越來越擁擠的市場中凸顯自己的特色。能夠提供這樣的應用程式，又能避免'大象'攻擊的公司應該會有一個光明的未來。圖 3-11 至圖 3-17 為金融軟體領域的架構圖，表 3-2 為整合者網站。

圖 3- 11 前端軟體



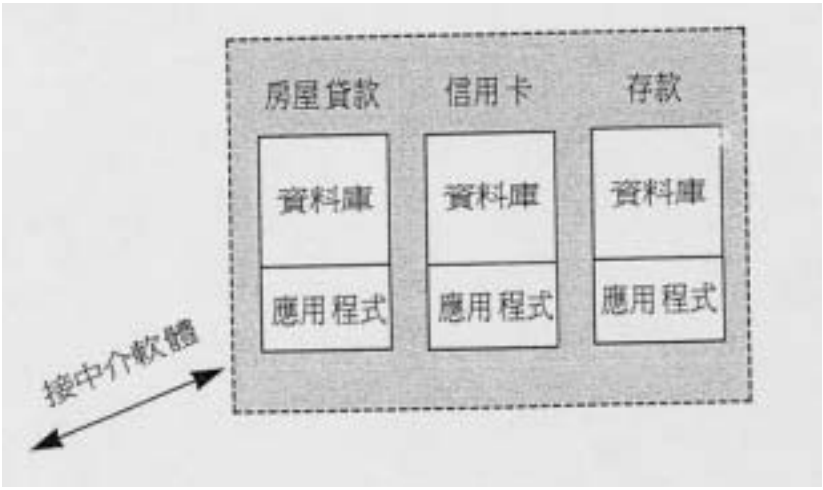
資料來源：參考書籍 R3（一）

圖 3- 12 中介軟體系統



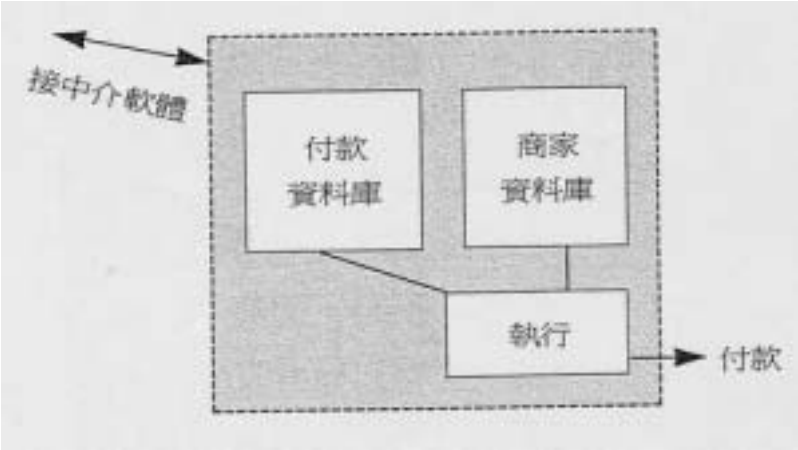
資料來源：參考書籍 R3（一）

圖 3- 13 中央處理系統



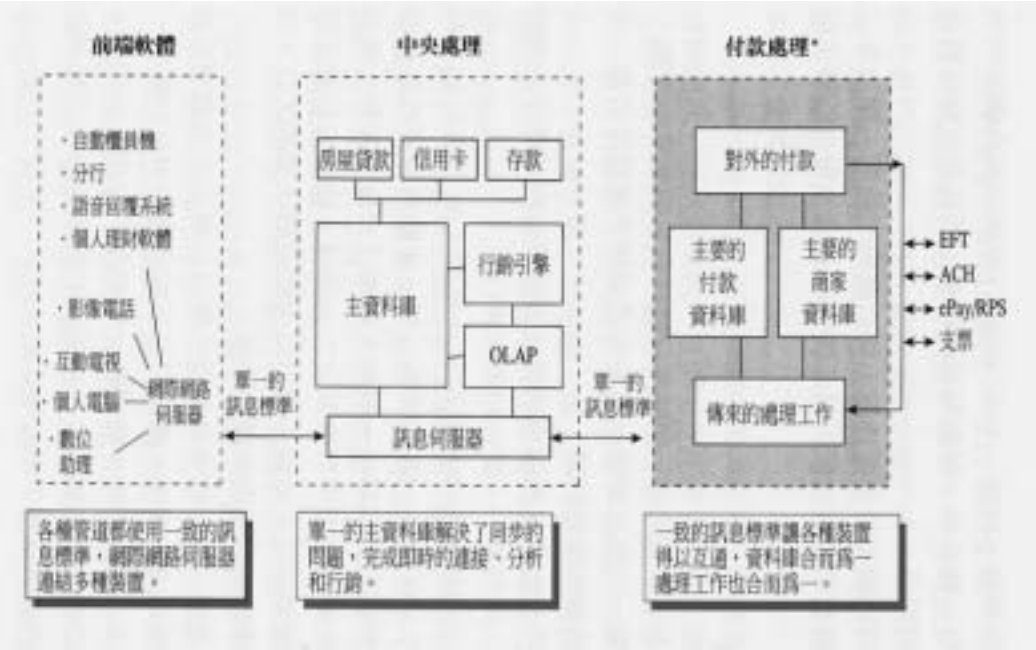
資料來源：參考書籍 R3（一）

圖 3- 14 電子轉帳繳費



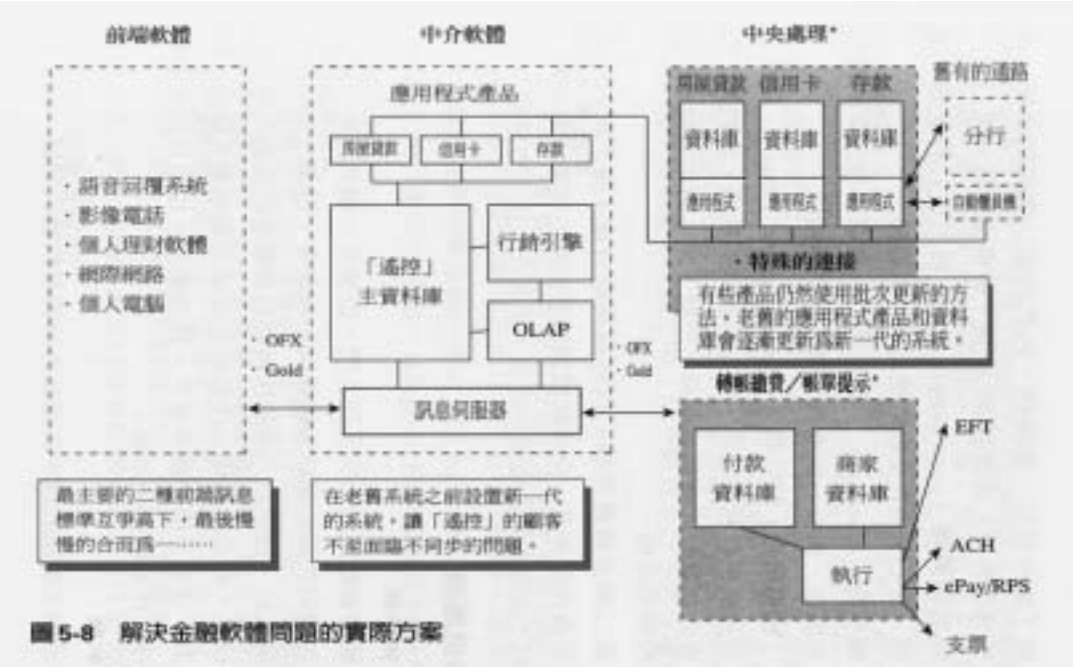
資料來源：參考書籍 R3（一）

圖 3- 15 解決金融軟體問題的理想方案



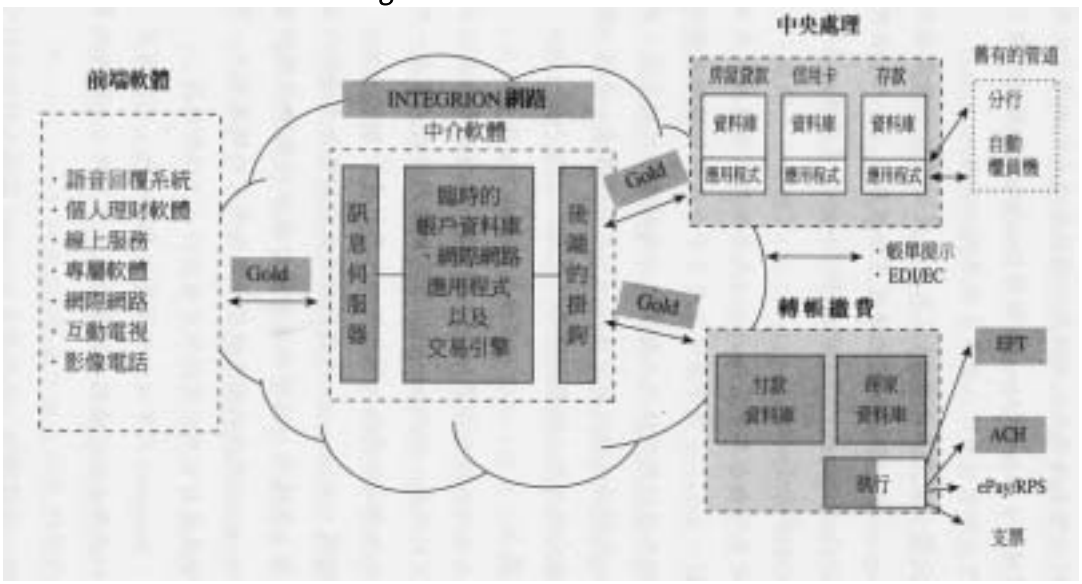
資料來源：參考書籍 R3（一）

圖 3- 16 解決金融軟體問題的實際方案



資料來源：參考書籍 R3（一）

圖 3- 17 integrion 在金融軟體中所扮演的角色



資料來源：參考書籍 R3（一）

表 3- 2 整合者網站

公司	網站	說明
美國線上	Personal Finance Center（個人理財中心）	個人理財中心是美國線上最受歡迎的服務之一。目前提供投資組合追蹤、信用卡對帳單、線上銀行和線上交易服務。透過 OFX 可以讓美國線上整合所有的資料。
Block Financial	Conductor	隸屬於 H&R Block 的網站，H&R Block 是 Compuserv 的母公司。和社區銀行合作，讓銀行的顧客可以與大型的投資公司進行「整合式」的連接，另有自營的線上信用卡和個人貸款服。
Intuit	Quicken.com	提供 Intuit 顧客投資、節稅和保險等方面建議的網站「整合」。與奮揚和美國線上有聯盟的關係。
微軟	Investor	結構上是微軟網路服務（Microsoft Network Service）的一部分，但也可以透過際網路連接。目前以投資服務為主，但誰也無法阻止它跨足其他金融服務，正計畫透過這個網站傳遞 OFX 對帳單。

資料來源：參考書籍 R3（一）

第四章 現行電子商務相關之風險管理機制與架構

第一節　企業電子化衍生的風險

企業電子化的風險有些是前所未見，如新產品、新服務與新市場衍生的促銷與支援問題；公共網路衍生的安全疑慮；網際網路衍生的稅賦與法律問題等等，不一而足。

既有的風險也會因為擁抱企業電子化而升高，包括如何有效掌控與管理核心事業的作業。如何讓營運和網路一樣，維持數小時不打烊，栽培員工的技術等。

雖然大家慣以負面的態度看待風險，不過危機也是一種轉機。在21世紀電子化的環境，沒有經過風險的粹鍊，企業無法掌握這個脫胎換骨的契機。

一、策略方向

企業電子化的提案成功與否，和企業擬議策略與落實策略的能力息息相關，即使公司的企業電子化還在剛萌芽起步階段，但若發生通路衝突，策略的好壞足以成就或拖垮整個公司。為了降低失敗率，擬議策略時必須清楚點出企業電子化對公司各領域有哪些正面的幫助。

支持企業電子化的戰略計畫，應該找出與現階段作法的落差，然後利用質化與量化的方式，小心翼翼擬出解決落差的辦法，並列出改採企業電子化後的好處。不妨逐一比較各種可行的作法，藉此評估各種作法潛在的衝擊，然後精心擬定一套評估標準，評比各作法的優劣，以提升計畫的成功率，降低失敗的風險。

考慮利用企業電子化改善銷售通路的企業，其所面臨的挑戰相當可觀，而其涉及的風險(包括領導階層是否能全盤了解策略方向的本意、能否擬出健全的計畫、是否有足夠的後援因應等)也非常棘手。不過利用企業電子化改善採購通路的過程就沒有這麼複雜，牽涉的風險相較之下也低了許多，所以不少大型企業的企業

電子化會從這裡出發。

在電子化的價值鏈裡，策略計畫不夠周延可能衍生的風險之所以受到高度重視，在於隨著進入外部企業體的公司的增加，接觸到失敗例子的機會也提升。

從企業電子化的觀點而言，策略計畫必須指明在整個企業的 IT 基礎建設上需要哪些主要之元件。藉由這樣的架構，企業才得以在電子化的道路上穩健地大步向前。此外，此階段也必須找出潛在的合作夥伴，以利後續向外的發展。

若公司未仔細規劃即草率進行企業電子化計畫，失敗率會相當高。總之在企業電子化的腳步擴及整個企業之前，必須顧慮到時間、財力與人力，一旦這些都俱足之後，企業電子化自會水到渠成。

舉例而言，若業務與客服部門之間的步調還是無法一致，就貿然對供應鏈大做改革，將可能嚴重影響到若干潛在性價值鏈條件日後的整合。

高投資報酬率是驅動企業電子化計畫的重要推手。不過確實掌握企業電子化計畫的總成本並不容易，而初期企業電子化的成效也許並無法立刻彰顯。然而業者應該小心翼翼。切勿忽視錯誤決策或完全不進行任何企業電子化行動所耗損的機會成本。

二、安全

安全在企業電子化的世界，若少了有效的安全措施，無法取信於人。滴水不漏的安全網需要精密的技術與萬全的流程支援，以便進行身分辨別、認證、授權、不可否認性、隱私保護和落實責任制等。

光是和客戶自動連線就潛藏可觀的系統與資訊上的風險，再加上整合需要以資訊為基礎的協同合作，與伴隨而來的安全疑慮，電子化企業領導人所面臨的挑戰更是雪上加霜。

透過風險管理可降低企業電子化的安全風險，此時更需要善

用企業電子化科技，確保以網際網路為基礎溝通的專屬性與有效性。

三、聲譽

公司的聲譽既多變又難捉摸，在網路世界更是如此。短短 5 年前能預見「虛擬」競爭者的出現?然而現今，隨著電子化企業概念的發展，網路事業更是蓬勃發展。

四、營運

營運是使企業電子化上路的主因，不外乎是簡化採購流程以及覬覦結盟後潛藏在營運的豐富商機。商機大多衍生於與營運相關的過程，而這些造成公司需要仰賴其他的外部供應商，來滿足自身生產製造上的需求。

企業電子化面臨的營運挑戰之一是專業技術人才供不應求。隨著企業電子化漸被業界採用，專業技術人員越來越難尋，內部人才的培訓不見得是萬全之道，因為一旦這些少數的「專家」被其它公司重金挖角，公司將陷入危險。為此公司應有充分的備用資源與應急計畫，不斷測試找出系統潛在的瑕疵，少了適當的防護網，可能讓公司毀於一旦，例如拍賣網站電子海灣在 1999 年年初，5 天之內當機 3 次，導致股價重挫 18%。擘畫未來電子化專案時必須量力而為，尤其是在營運上，否則企業電子化的腳步上成長太快，即便是最有活力的生產環境也會吃不消。此外，控管變化機制的成立有其必要性，以將電子化計畫對營運可能造成的風險一一提出來和組織的方向比對一番。企業電子化的提案不只是 IT 的問題而已，也是策略計畫，需要公司各部門通力支持。

五、人力資源

人力資源部的首要作用，是協助員工適應電子化後角色與權限劃分，人力資源部門必須訂出一套辦法，協助降低電子化提案的進行。鬆散的組織架構有助於抒緩新角色造成的恐慌。公司高層必須帶頭示範全力支持電子化專案，並展現自信、胸有成竹的

感覺，以安定員工浮躁不安的心。人力資源部門也必須是驅動終身學習的火車頭。電子化計畫上路後，員工的角色與責任不斷擴大，具備十八般武藝不僅重要也是必要條件。若公司有正確的專案管理流程、妥當的組織架構和多職能的員工，電子化計畫成功的機率才會大增。延攬人才是許多企業的首要之務，具備管理電子化專案能力的人才難尋，因此企業大方祭出利多，以積極網羅並留住好人才，以免重要部門出現人才荒，影響公司營運。此外，面對激烈的挖角風，人力資源部門必須以創新的手法促銷公司，並想辦法營造可讓員工寓工作於樂的環境。

第二節　風險管理概要

一、風險的本質與管理

風險有許多不同的定義，其中最普遍一種就是不確定性。在投資理財的世界中，風險可以視為對未來的不確定性。當投資人不能確定其投資的報酬率時，便面臨風險。絕大部分的投資行為都牽涉到風險，例如投資股票或債券時，無法確知下一期股價或報酬率會是多少。當然，無風險的投資也存在，例如定存。只要存入的銀行不倒閉，投資人就可於期初確知期末的收益，但這類投資畢竟屬於少數。現實世界中，牽涉到風險的事情遠多於百分之百確定的情況。

由於風險反映未來的不確定性，它是一個事前的概念。我們對於未來報酬的預期，一旦損益發生後，就屬於風險的實現。本節的主要目的，就是在引領讀者於損益尚未實現前，對風險有正確的評估與控管，以避免承擔超過預期的損失。

許多人將損失與風險混淆，總認為發生損失，才算是風險。其實就上述定義，將風險解釋為報酬的不確定性。只要不確定性增加，不論預期報酬上升或下降，都是風險提高的表現。因此只要報酬改變的幅度增大，就視為風險增加。在這種定義下，損失固然是風險，但異常的報酬增加，也反映風險。因此風險並不一

定代表損失，而是報酬的不確定性增大，導致虧損的幅度或機率增加。

風險與報酬經常相提並論。事實上，風險與報酬是投資的一體兩面。人性偏好高報酬，確定的高報酬則更具吸引力。對於不確定性高的投資標的，投資人會予以折價，期初的折價使得風險較高的證券於整段期間的報酬相對提高，持有者以較低價格取得，因此風險與報酬兩者之間，高報酬通常伴隨著高風險；而低報酬的投資工具, 其風險也比較低。比較電子股與傳統產業股票，電子股的長期報酬較高。但是在相同市場狀況下，電子類股的報酬波動性也比較高，因此我們可以說電子股是一種高報酬，高風險的股票。投資人若想享有較高的長期報酬，必須承受相對的短期波動，然而在市場狀況不佳時，高風險股票的跌幅往往大於低風險的股票，這時就是其風險實現。喜好高風險的投資人也不用過於驚訝，但必須強調的是，經過一段相當長期間後，高風險的股票平均報酬應該會較高。如果高風險的股票不具有較高的預期報酬，投資人將不願持有，預期報酬較高的部分是投資人承擔風險的補償 。

風險有程度上的差別。不同的證券種類、類股、以至個股都有其所屬的風險水準。投資人可依其願意承擔的風險水準來選擇投資標的。一般而言，公債的配息固定，違約機率又小，故風險最低，公司債包含較高的違約風險，股票的收益不固定，股東對公司的求償權又次於債權人，故風險較債券都高，衍生性商品如期貨、選擇權和認購權證的風險又更高。長期而言，預期風險愈高的證券提供愈高的期望報酬，一些企業則企圖對風險加以控管，並積極地調整其風險曝露。藉此發展相對競爭力，不論採用何種態度面對風險企業都必須了解風險管理的重要性，並且具備相當程度的風險意識。

風險管理是釐清各種風險因素，衡量風險曝露以及控制風險的過程。著名的財金作者伯恩斯坦在「與天為敵」一書中，細數人類有史以來對風險、不確定性與機率的了解和發展。人類逐漸

從數學與機率的推演中了解到，許多事情之所以發生，並非天命註定，而是機率下的產物。在某些條件與情況下，我們甚至可以預期事件發生的可能性。有這種認知，風險管理的觀念便逐漸形成。各種溝通科技的發展，包括電話、電訊和網路，將全球市場緊密的連在一起。同時也將一個地區的波動性，快速地傳達到另外一個地區。

二、風險管理的技巧

風險管理是一項十分複雜的工作，在瞬息萬變的網際網路世界中，許多企業內在與外在的因素都是我們無法控制的，因而風險管理也逐漸受到企業的重視。風險管理在發展電子商務與推動企業 e 化的過程中，企業會遇到許多的障礙。不論硬體、軟體或人員，企業都必須清楚的瞭解潛在的失敗因素，並利用有效的策略來降低風險。每個企業都應該根據其企業文化經營型態，制定屬於自己的風險管理機制，而一般最基本的風險管理概念包括：評估執行的成本與效益，並藉由多種解決方案來降低風險，評估做與不做之間的風險，而不只是要怎麼做的問題；評估對企業的影響，有效分配內部資源與外部資源來執行工作。

三、風險管理的步驟

風險管理包括確定、評估與管理三大步驟，風險包括人事、需求、技術、商業等複雜的組合。找出可能的潛在風險，就是風險管理的第一步。要評估電子商務與企業 e 化的風險十分困難。一般來說，可藉由顧問或有經驗的人獲得，定期評估可以有效防止潛在風險，而不會等到事態嚴重的時候才發現。預防風險最好的方法就是妥善的準備、定期評估、溝通與改善，也是降低風險的不二法門，而有效的知識管理策略更是預防風險的利器。

第三節　現行風險管理的機制與架構之檢討

一、消費者擔心的隱私和機密問題

關於隱私的關係，商業和政府必須長久收集保存顧客及公民個人的機密資料。但是，網路急劇改變了這種情形，引起重要電子改革，電子支付服務的公司和提供電子資料庫的供應商，在網路上做儲存資料分析的處理。

這些電腦化的活動，透過直接聯繫可以將這些事務處理完善。但是，由於種種原因，也可能發生資料的分享，例如：為銷售目的，把這些資料傳給其他商業團體，或為了計算稅金，把這些資料傳給政府。

由於資料的普遍收集和使用，消費者開始關心個人的隱私是否保密。根據聯邦貿易委員會在美國國會提供的一篇證言指出，92％的美國人關心他們的個人資訊是否在網際網路上被濫用。這個數據間接顯示出駭客的活躍，駭客試圖透過網際網路勒索金錢。時代雜誌報導，駭客在網上郵寄了 300,000 個信用卡片，造成成千上萬個網路顧客的秘密資料外流。

（一）存取

網路消費者應該選擇可辨認的資訊，並且加以控管。消費者在存取資料後，應該能夠複查關於他們自己的資訊是否正確。

（二）安全

充分而完整地保護消費者的秘密資訊，並且禁止侵害使用者的隱私權。

電腦可以儲存和收集個人的資料，對資料若不加以控管容易侵犯到使用者的權利。以前曾發生醫院存取電腦系統，獲得著名人士的醫療記錄，再賣給小報記者的事件，造成許多財政機構、電子商務零售商和健保企業的不便。尤其是有關顧客或病人的巨大資料庫的秘密資訊。

二、電腦處理個人資料保護法頒布

1999 年美國國會制定 Gramm –Leach-Bliley Act (GLB)。GLB

要求財政機構嚴加保護消費者非公眾資訊的安全和秘密。除了GLB 外，還有 13 個現存的聯邦法，彼此並不互相取代，在所有50 種狀態中，實際提出秘密考慮，分類如下：

（一）加拿大

在加拿大，關於消費者隱私權、個人資訊保護和電子簽章的法律也是有所變化。前不久才加入國際外科醫生協會文獻行為的相關條文，其他權限的立法大部分主動加入了加拿大隱私權法律，特別是關於個人隱私權的保護上。加拿大法律保護個人的私人秘密資訊，為聯邦政府商業選擇電子商務和澄清如何使用電子商務的依據。

（二）歐洲協會

在歐洲協會，對資料保護也有相關規定。在歐洲聯盟之內從事個人資料的處理必須遵守包括財政機構和所有企業堅持的八個原則。這八個導引原則為合法處理個人資料、遵從協會的規定、合法獲得個人資料、個人資料要充分、個人資料的更動時時修正、個人資料保有的時間、應該依據個人權利處理個人資料、個人資料應該用於技術和組織的測量、避免未經許可不法處理或偶發的損失、破壞和損害個人資料。

（三）澳洲

澳洲共和國在 1988 年制定了隱私權的法律。目前，秘密行為侷限於公眾部分，然而，秘密修正案（私人部分）在前不久也列入法律中。修正案的目的是要求部分私人機構盡到國家秘密原則大綱中的 10 個責任。

現在澳洲沒有合法託管資訊安全的合法標準。然而，AS/NZS 4444 以資訊安全管理為基礎，是目前最好的工業領導。它主要為了改善商業和消費者對網路安全缺乏信心的問題。

（四）香港

在香港，由個人資料秘密法令構成的全面保護網，管制個人資料秘密。法令根據他們的個人資料，保護個人的秘密避免被誤用和盜用。法令提出個人資料的安全和合理實行的

步驟，確保個人資料未經許可外流

三、全球的連線問題

網路犯罪的範圍已經擴大到全球，其手法以非傳統的國際犯罪。沒有國際邊界，駭客能夠在電話和網路中隱藏，更易於犯罪。

當使用者鍵入命令獲准進入網站時，駭客不需要護照也不用透過檢查點，便可以舒適地從家中匿名工作，輕鬆拷貝他人的資料。更甚者，駭客能夠破壞顧客在商業上的秘密和其他形式的資訊。在這個容易犯罪的網路世界中，監控上的弱點給駭客無限的機會，使得網際網路變成犯罪的完美工具。

大部分的人質疑，為什麼電腦犯罪沒有國際化的法令來約束？因為國際犯罪的預防程式，必須先有國際合作。美國是世界最主要的電腦化國家，系統連接到全國法官協會的電腦，而電腦化落後國家的相關法令卻很薄弱甚至缺乏，而成為駭客攻擊的主要目標。這對國際的合作是一個很大的障礙，在最近農村國家的考察中發現，有 33 個國家還沒有更新他們的法律，提出應對網路犯罪的法案，而充分或部份更新網路犯罪法律的國家僅僅只有 19 個。缺少國際幫助對網路犯罪的成功調查和告發是一個主要障礙。歐洲 G8 和委員會正努力使農村國家的電腦犯罪法律和國際調查合而為一。文明國家透過國際權限合法規則的差別，可以鑑別和保護重要的消費者。

電子簽章法的通過，可在合約規定的環境條件中，建立電子簽章的有效性。但是在沒有相關法律的農村國家，若無法產生這樣的簽章和從權限實體執行的電子設備，一個再好的網路安全計畫，也不能除去所有危險（換句話說，網路安全涉及危險的管理，事實上無法完全消除危險）。當需要調查時，它必須記得大多數以電腦為基礎的證據。無數電腦和電子資訊佈署的網路系統以保護社團利益為首要重點。電腦改變了商業的方式，電腦的濫用也給調查方法和公民與行政論文集上類似的衝擊。透過可靠的保存證據，從電腦提取資料不是一個簡單事情，很容易發生故意或意外

改變資料的情形。

人們開始精心地做「電腦辯論練習集」，分析儲存電腦可靠性，以提升取得電子證據的科技。的確，「電腦辯論練習集」程式提供許多民用和犯罪的電腦辯論練習，相對地這種練習必須建立在一個由許多硬體站臺和軟體應用的技術環境中。為了在這個環境中提取資料，辯論練習檢查員必須使用各種硬體和軟體的工具來加速複製、回顧和提供電子證據的過程。然而，如果沒有這樣的工具禁止電子犯罪將是不可能的。

認為只能夠把電子證據用於民事訴訟是有爭議的。如最近微軟的反托拉斯事件，律師回顧電子郵件的價值，和各式各樣合法電子證據的形式被限制在動態存儲中所存在的文件。但是，他們沒有因此被侷限，反而進一步尋求所有存儲的資料、刪除的文件、備用支援卡帶和文件的碎片等。尋求精確的證據，按科學的方法及法庭的規定可重複分析這些資料。

雖然磁碟可以被用來長期儲存資料、恢復磁碟的損壞或天然的災害，但是其中的資料涉及私人秘密（隱私）。內部的調查引起騷擾的抱怨，或者發生其他不規矩的行為時，法庭必須再次被消除電子郵件或者是其他的資料。在律師利用法庭的老舊電腦前，也必須以契約承諾守密。

雖然這些努力有可能會因為搜尋而導致電子證據民事或刑事的訴訟。因此，用來搜尋證據的工具和程式，必須像民事和刑事的訴訟人所使用的那樣可靠。合法而可靠的法庭工具，僅能用在內部的計調查。

除了大量導致刑事訴訟的工作，也有少數的調查是屬於私人部分，為加強法律達到快速實施的目的，這時，法庭可以委託公司或者外部電腦法庭的專家來完成工作。在電子處理過程中為可能發生的犯罪建立防止機制，例如犯罪者紀錄資料庫應拒絕外流，以扼阻犯罪意圖。同時犯罪者紀錄不應只記錄公司名稱，應記錄公司所有上層主管，預防公司詐騙。

第五章 國內現行電子商務風險管理之運作現況

近數年來，網際網路的熱潮與各類數位化的商機、層出不窮的服務與產品，成為未來知識經濟時代的新興範疇。網路上營業的電子商店，政府若無適當的法令及機構來加以管制及監督，消費者在網路上進行交易，因無法確認對方商家是否為合法營業，還是僅有網站的空頭公司，貨物交易的付款方式如何，商品的交貨情形如何...等等，在消費者心裏存在諸多的盲點，因無法只聽信網路上的片面廣告，就對網路商店達到百分之百全信的程度，完全毫無顧慮的進行消費，消費者的消費意願就無法提升。

相對的在電子商店商家的立場，也無法確認在網路上進行消費的消費者，是真正的網路上下單購買的消費者，還是網路上的駭客，或是網路騙子...等等，因為也無法保證商品賣出去，就必定能夠收到貨款，電子商家在千思萬慮之下，也無法對如此便利的網際網路（Internet）營運管道，擁有百分之百的信心，同樣也就無法全力對網路商店事業進行投資。

在網路商家及消費者都處於觀望的階段，雙方似乎都既渴望又怕受傷害，都在等待政府對於電子商務的制度政策做更周詳的規劃，以利用網際網路達到便民的功效。

第一節　電子商務之法律策略

一、電子商務之法律環境架構

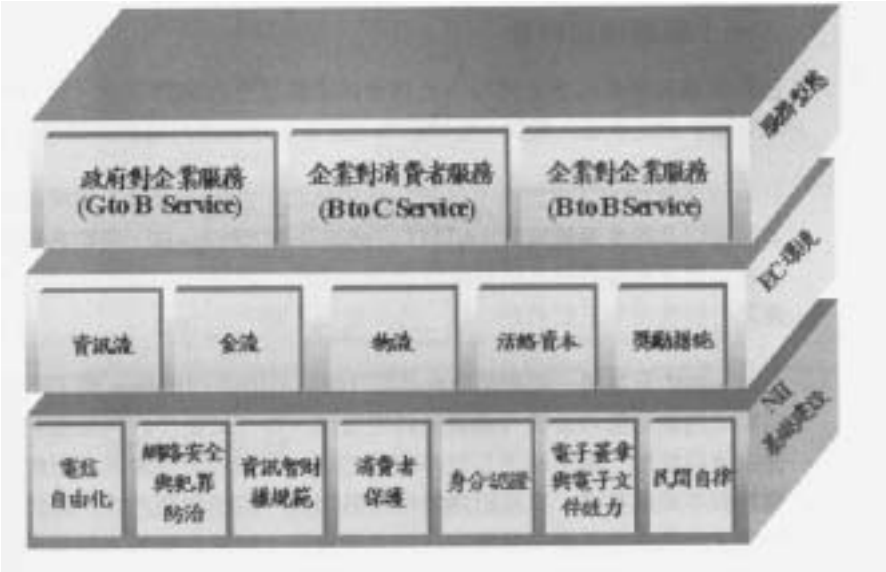
法律環境架構之建立乃是兼顧網路發展與社會利益，藉由建立一個網路交易與使用環境規範的最低標準，使網路使用者與企業經營者有所遵循，進而使網路使用者在此法律規範下的網路環境消費交易，或利用網路資源時有所保障;至於智權規範與保護乃是將實體世界中有關智慧財產之保護規定，進行適當的修訂或增訂，提供網路使用者或企業經營者在面對新興科技與網路環境

時，於使用著作、創作或其他智慧財產權時，能於促進社會利益與創新和著作保護之兩端點上有所平衡。

網際網路建設為電子商務推動基礎建設工作，為建立資訊網際網路良好發展環境，行政院國家資訊通信基本建設專案推動小組已積極檢討修訂相關法規。至目前為止，已研擬政府資訊公開法及數位簽章法草案。

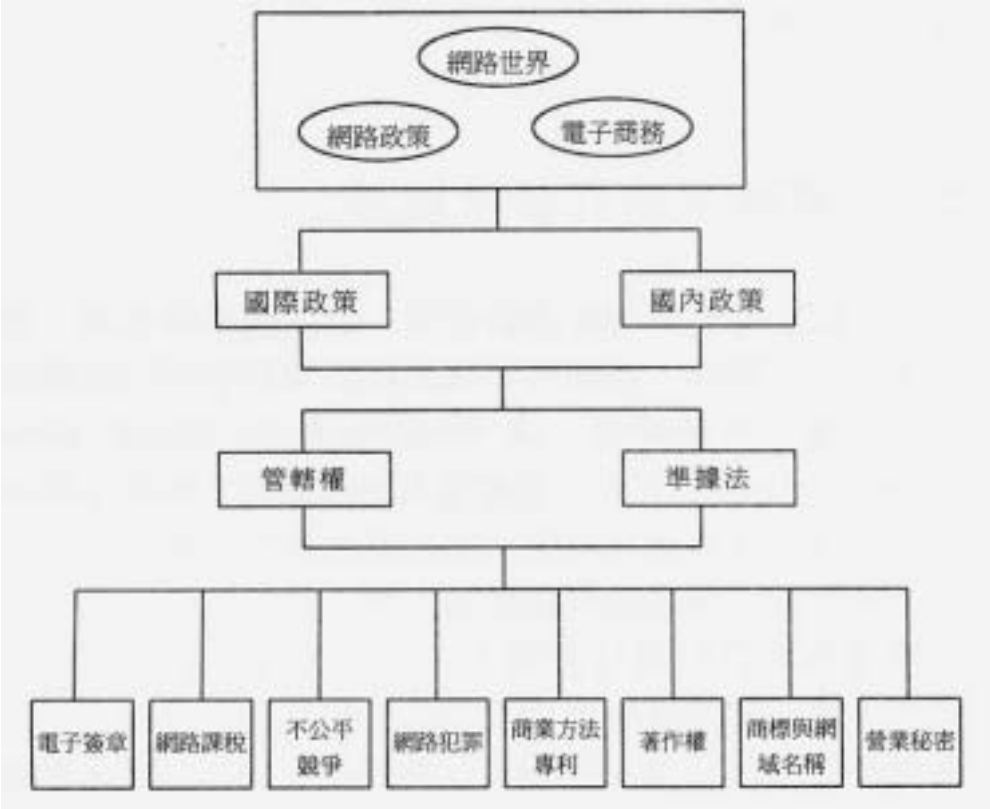
修訂刑法、電信法、有線廣播電視法、商標法、著作權法、仲裁法、電腦處理個人資料保護法、銀行法、所得稅法、稅捐稽徵法、營業稅法等十一項法律。同時檢討公平交易法、消費者保護法、貿易法、公司法及商業登記法、電子資金移轉法、洗錢防制法、證券交易法、關稅法等九項法律。同時積極建立電子認證制度，維護安全及可信賴之網際網路環境，輔導廠商建立電子交易契約一致性規範，以預防糾紛。圖 5-1 為相關法規與網路基礎建設的關係圖。圖 5-2 為網際網路與電子商務衍生出的相關法律課題。

圖 5- 1 法規與網路基礎建設



資料來源：資策會

圖 5- 2 網際網路與電子商務衍生的相關法律課題



資料來源：參考書籍 R2（十一）

二、各國電子商務之立法現況

歐美等主要國家為建立安全及可信賴的電子通信及交易環境, 普及電子商務之應用, 早已積極致力推動電子簽章法之立法, 例如, 德國(1997 年 8 月)、馬來西亞(1997 年)、義大利(1997 年 3 月)、新加坡(1998 年 6 月)、韓國(1999 年 7 月)、香港(2000 年 1 月)、日本(2000 年 5 月 24 日)以及美國各州(已有四十餘州完成立法)。美國聯邦電子簽章法則是 2000 年 6 月由參眾兩院審議通過, 柯林頓總統完成簽署公布程序, 完成立法工作。歐盟組織亦於 2000 年 1 月完成電子簽章法指令之制定, 各會員國均須依據指令之規範, 在 2001 年 7 月前完成會員國內國法律之調和。積極進行電子簽章相關領域之立法的國家, 有英國、法國、加拿大、澳洲等。

以歐盟為例，歐盟於 2000 年 1 月 19 日公布電子簽章法指令(Directive l999/93/EC of the European Parliament and of the Council of l3 Dec.1999 on the Community Framework for Electronic Signatures)。這項指令並非針對電子簽章進行嚴格管制，而是就電子簽章做出定義與規範其法律效力，並就提供憑證服務應具備之條件加以規範，提供最低限度的安全性。各會員國均須依據指令之規範，於 18 個月內, 在 2001 年 7 月 19 日前完成符合指令規範國內之法律、規則與行政措施等法律。為因應電子簽章之快速發展，委員會(Commission)應考量科技、市場與法律等發展情形，檢視本指令運作情形，並評估各會員國運作的和諧性(harmonization)，最遲於 2003 年 7 月 19 日前向歐洲議會與理事會(European Parliament and the Council)提出報告，這項報告得以提出法律草案方式進行。

歐盟電子簽章法指令立法目的在於便利電子簽章之使用，並提供其法律地位，且藉由建立電子簽章與憑證服務(certification services)之法律架構，確保內部市場的妥善運作。對於電子簽章，歐盟在指令第 1 條賦予其法律上的承認，不能僅因其(1)以電子形式存在;或(2)不具備合格憑證(qualified certificate);或(3)憑證是由未經許可之憑證服務提供者所簽發，以及(4)非由保全簽章產生裝置所產生等原因，而逕行否認其法律效力與訴訟程序之證據適格性。若電子簽章是基於合格憑證與依保全簽章產生裝置所產生之高階電子簽章(advanced electronic signature)，則其效力應等同於法律所要求之簽名，並可作為法律程序之證據。

所謂高階電子簽章，是指該簽章符合(1)與簽署者(signatory)間為唯一的關聯；(2)能證明簽署者身分；(3)在簽署者專屬控制(sole control)下，利用簽署者維持的手段所創造出來的；(4)與資料相關聯，此關聯性指資料若有實質變動則可察覺等規定之電子簽章。

歐盟電子簽章法指令通過後, 於 2000 年 5 月 4 日正式通過歐盟內部市場電子商務資訊社會服務法律觀點指令(European parliament and council directive on certain legal aspects of information

society services, in particular electronic commerce, in the internal market)，該指令要求各會員國排除使用電子契約之限制或禁令。此外，在電子契約締結時，透過特定資訊的要求，以確保法律安全，尤其是幫助消費者避免科技錯誤。並符合歐盟電子簽章法指令之規定。這兩項指令的實施，使得歐盟在建構電子商務法制環境更趨於完善。

三、我國立法背景與現況

台灣民法第 73 條前段規定，「法律行為不依法定方式者，無效」。所謂法定方式(法定要式行為)，亦即意思表示需依法律規定之方式作成，例如以書面作成。這些規定散見於民法、海商法、證券交易法、票據法、公證法、破產法、公司法等。因此，電子文件並不能符合現有法律規定之書面要式，唯有藉由電子簽章法之建立，才能因應網際網路與數位經濟活動廣泛使用電子文件之需求。

為配合 NII(國家資訊基本建設)之推展，台灣於 1997 年由經濟部委託資策會科技法律中心進行數位簽章法之研究，並建議儘速研訂數位簽章法，訂定電子簽章及電子文件之法律地位，建立電子憑證機構(Certificate Authority, CA)之管理制度，界定憑證機構與使用者之權責，建立跨國認證之機制。由於數位簽章法是一新興的科技立法，行政院 NII 小組決議組成「數位簽章法研擬小組」，負責草案研擬工作。研擬小組於 1998 年 1 月成立，參酌主要國家之立法經驗，以及參考聯合國及歐盟等國際組織之電子簽章立法趨勢，研訂電子簽章法草案。後於 1999 年 12 月完成「電子簽章法草案」之研訂，經過行政院第 2061 次院會正式審議通過。送交立法院。立法院於 2000 年 3 月 28 日完成一讀程序。現正交付相關委員會審議中。依照電子簽章法草案之前言，台灣的電子簽章法立法有三大原則：

（一）技術中立原則

任何可確保資料在傳輸或儲存過程中完整性及鑑別使用

者身分的技術，皆可納入使用，並不以「數位簽章」為限，以免阻礙其他技術應用發展。制定法律應採「電子簽章」法為立法方向，而不以「數位簽章」法為限，以利日後諸如生物科技等電子鑑別技術之創新發展。也就是任何電子技術製作之電子簽章及文件，只要功能與簽名蓋章、書面文件相當，皆可使用。

（二）契約自由原則

對於民間之電子交易行為，宜在契約自由原則下，由交易雙方當事人自行約定採行何種適當之安全技術、程序及方法作成之電子簽章及文件，作為雙方共同信賴及遵守之依據，並作為事後相關法律責任之基礎，政府不宜以公權力隨意介入交易雙方契約關係，交易雙方應可自行約定共同信守之技術作成電子簽章及文件。另憑證機構與其使用者之間，亦可以契約方式規範雙方之權利及義務。

（三）市場導向原則

政府對於憑證機構管理及電子認證市場發展，宜以最低之必要規範為限。電子認證機制建立及電子認證市場發展，宜由民間主導發展各項電子交易所需之電子認證服務及相關標準。

行政院電子簽章法草案規範的適用範圍顯然大於一般的電子商務。包含了公、私領域。如政府的公文傳遞、民眾辦理戶籍登記、繳納稅款，或私人之間的交易或文件的往來，其目的在於建立電子認證制度、增進電子通信及交易的安全。除行政院版本外，若干立法委員也提出各自的版本草案，進行併案審查。

四、相關法令的修改

建立安全及可信賴的網路環境，確保資訊在網路傳輸過程中不易遭到偽造、竄改或竊取，而且能夠鑑別交易雙方的身分，並

防止事後否認的情事，是電子化政府及電子商務能否全面普及的關鍵。在電子簽章法一旦通過立法。政府相關單位必須及時研擬出那些法律行為不得以電子文件為之，避免日後爭議叢生。此外，電子簽章技術對於一般民眾而言屬於新興科技，在使用上可能會產生疑慮與排斥。雖然電子簽章法並未要求某些特定行為，必須以電子文件為之，當事人可以依照契約的約定，決定是否使用電子文件或電子簽章，然而民眾的訓練與宣導是必要的。目前政府及民間企業正致力於利用現代密碼技術，建置各領域的電子認證體系，提供身分認證及交易認證服務，以增進使用者的信心。

五、國際間電子商務相關作法

（一）美國聯邦政府 EC 工作小組年報（89.2.1/89043067）

重申 1997 年美國克林頓總統對電子支付系統指令，其認為財金主管應多與外國政府合作，以便監督新開發電子支付系統經驗，反對政府使用不具彈性及以高度管理規範企圖制止新電子支付系統開發。並說明電子聯邦稅支付系統（EFTPS）之附加利益，並提及政府內部電子交易、卡片服務、對公眾之安全的銷售、電子檔案、電子支票及儲值卡辦理情形。

（二）美國與智利簽署雙邊 EC 聯合聲明（89.2.29/89073932）

電子支付部分：應確認電子付款是由私部門主導，並應提升彼此之競爭市場及使用者信心。

（三）紐西蘭發表電子商務發展策略報告（89.5.11/89170965）

紐西蘭發表之電子商務發展策略報告之主要內容分為立法架構及保護消費者權益、探討經濟及社會衝擊、政府歲收、安全課題、電子化政府五大部分，其中安全課題乙節，包括認證法制及建立互信基礎、跨國交易、數位簽章法效及安全與隱私問題，該國認為對電子商務發展其所持最佳立場：

1. 密切注意其發展。

2. 保持對科技及應用之高度認知。

3. 利用科技以補強政府傳輸服務。

4. 準備適切的立法或監理措施。

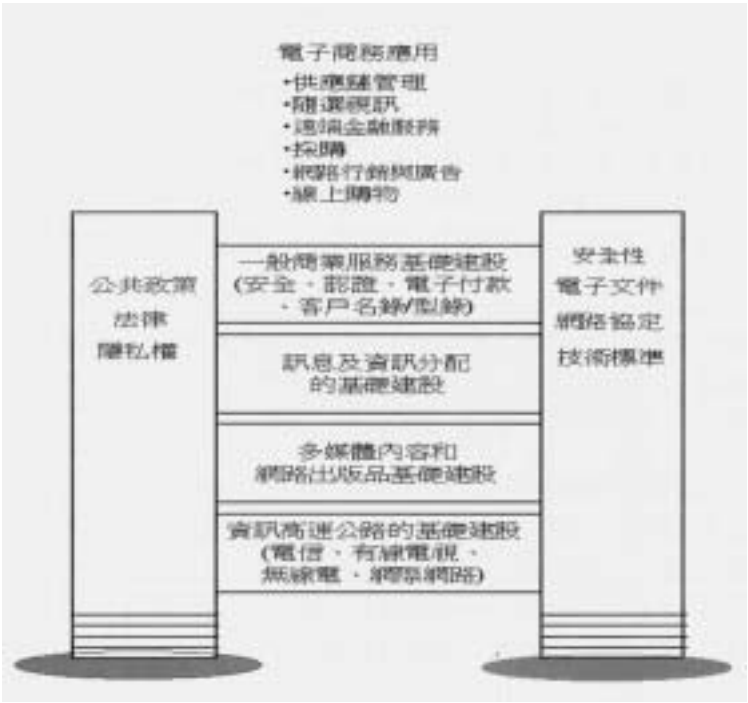
（四）歐盟執委會通過電子商務指令修正草案經歐洲議會於本年五月四日通過電子商務指令（89.6.7/89205623；89.6.15/89217176）

金融服務方面，指示金融服務應利用網際網路提供各項銀行現有全部既存業務，以縮短銀行與消費者間距離。議會並支持金融服務業保有對原提議以不減損銀行既有提供服務項目（並含不減損有關消費者契約之義務）之共同立場，該立場尚無擴大其範圍，乃應就個案提出。

第二節　國內現行電子商務之運行現況

一、電子商務基本架構

圖 5- 3 電子商務基本架構



資料來源：經濟部商業司

電子商務一般是指：「利用 Internet 所進行的商業活動」皆可謂之為電子商務 (Electronic Commerce 或稱電子交易)。電子商務整體交易環境架構係包括消費者、電子商店、金融單位、安全認證中心等，其架構如圖 5-3。

根據 Kalakota & Whinston 1997 年提出對電子商務的看法是：兩方或多方通過電腦和某種形式的電腦網路(直接連接的網路或 Internet 等等)進行商務活動的過程。主要是用來改善與客戶的互動、企業流程、企業內和企業間資訊的交換。

電子商務這個概念起源於七十年代。當時一些大公司通過建立自己的電腦網路讓各個機構、商業夥伴之間的資訊共享，這個過程被稱為 EDI(電子數據交換)。EDI 通過傳遞標準的數據資料可以避免人為的失誤、降低成本、提高效率，據估計在世界 1000 個最大的企業中，95 以上的曾使用這一技術。它過去是、現在也是電子商務的基礎。

Kalakota & Whinston 對電子商務提出的一般架構，如圖 5-3 電子商務基本架構圖所示，此架構包含了：

（一）兩大重要支援支柱:即公共政策(如電子簽章法案)與技術標準(如 TCP/IP通訊協定)。

（二）一般商業服務基礎建設:包含安全、認證、電子付款、電話簿與型錄等。

（三）訊息與資訊分散基礎建設: 包括了電子資料交換、電子郵件與超文件傳送。

（四）多媒體內容與網路出版基礎建設：包括超文件標示語言、爪哇語言、全球資訊網和 XML 等。

（五）網路基礎建設：包含電訊、有線電視、無線電與網際網路的基礎建設。

根據電子商務的一般架構，電子商務必須在公共政策與技術標準的制定下。建立一般商業服務、訊息與資訊分散服務、多媒體內容與網路出版服務及網路之基礎建設，才能夠提供供應鏈管理、隨選視訊

等電子商務的應用。

二、我國電子交易現況

（一）電子金融業務概況

1. 推動金融卡片業務(截至八十八年十二月底為止，全國自動櫃員機幾近一萬四千台，金融提款卡之流通數達四千一百萬張，透過自動櫃員機之交易金額更高達五千五百七十七億元。)
2. 推動金融電子資料交換業務(平均每月交易量達一十二萬筆，交易金額達一百三十八億元)
3. 推動電話銀行及個人電腦銀行(我國電話用戶已逾九百多萬戶，行動電話亦逾百萬戶，目前本國銀行均已提供該項業務，推動網際網路電子銀行之業務(已核准多家金融機構開辦網際網路電子銀行之業務)。

（二）主管機關應重視問題：

1. 網路交易安全問題
2. 確保消費者權益問題
3. 金融體系認證作業問題
4. 網路交易風險管理問題

（三）推動策略

1. 金融業電子商務金流作業規劃由金融業主導。
2. 金融業應與其他產業間建立有效互動機制。
3. 督促銀行公會成立「電子商務金流作業研究暨推動專案小組」，專責辦理電子商務金流推動工作。
4. 推動各金融機構建置金融電子資料交換（ＦＥＤＩ）系統功能。
5. 推動各金融機構建置網路銀行系統功能，結合其他各類型加值網服務，建立網際網路金流服務通道。

6. 在符合競爭機制下，研究發展我國金融體系之領袖認證單位（Root CA）。
7. 金流部分：金融局亦配合行政院產業自動化及電子化推動方案研訂「推動金融業電子化計畫草案」。
8. 積極參與訊息標準(UN/EDIFACT)之國際會議，以掌握訊息交換作業。
9. 隨時檢討安控基準，確保網路交易安全。
10. 加速金融服務網路化之推動，簡化網路銀行作業之核准作業。
11. 重視客戶隱私權保護。
12. 配合電子商務發展積極推動無紙化之金流交易環境。

第三節　電子商務之風險管理政策

公元 2000 年 3 月網路駭客引爆的「阻斷服務」（Denial of Service；DOS） 事件，不僅癱瘓 Yahoo、Amazon 等諸多大型網站，更導致全球股市下跌。2000 年 5 月，一封「I LOVE YOU」挾帶意想不到的情書病毒，造成破天荒的損害。2001 年 5 月中美駭客大戰，雙方號稱攻佔對方多個網站。以上幾種觸目驚心的事件，加深政經業界單位對資訊安全的焦慮。不過國際電腦安全協會（ICSA）指出，其實 60%的洩密事件來自企業內部，僅有 15%來自外部。所以資訊系統應有一套完整的風險思考及安全架構，再從可接受的風險管理角度，決定主要必備的安全防範措施。

資訊安全有許多種表達方式，考慮資訊安全威脅，可把資訊安全內容分為設備、軟體、資料、個人及企業經營需求等幾個部分。資訊安全的主要威脅或弱點，來自資訊資源本身或使用的介面。不安全事件的發生有前因和後果，也就是輸入（前事件）和輸出（後事件），伴隨輸入和輸出而來的便是風險。本文即是要利用風險管理的分析方法，提供相當的防護與保險，將意外對政經業界單位組織的傷害減到最小。

資訊安全的風險管理分析方法包含「風險評估對象」、「風險辨認」、「風險估計」及「風險控制策略」四個程序。「風險評估對象」是企業在面對資訊系統時，應先確定那些資源或事件會產生威脅或弱點。「風險辨認」蒐集各種可能威脅資訊安全的有關資料，通盤分析以確認危險所在。「風險估計」則在評估風險事件的發生機率，瞭解可能引發的損失，作為風險衡量準則。「風險控制策略」是定義可能影響的衝擊，作為資訊安全決策的參考，建立有效、適用的企業安全政策。

一、風險評估對象---評估哪些資源或是事件具風險性

電子商務面對大量資訊技術的使用，與企業營運之管理、工作方式與文化產生變革與衝突。經營者面對的挑戰，在於過往透過人工做流程設計與授權，以及藉由各類的資料庫與資料處理來描摹企業的藍圖，以達成經營決策。此等營運競爭的價值鏈，隨著網路化技術與資訊化工具的大量導入，遭遇到難以掌控的挑戰，甚或原有對控管的認知均不適用於網路化後的環境。所以如何將原有經營者的管理融入現代化科技工具之內，為目前使用各類網路化技術（如 ERP、E-Business、SCM、CRM 等）之企業不得不面對之課題。

由於資訊系統的導入，使得部門營運都具體而濃縮至資訊系統內部，而企業營運的實際情形，均通過資料庫內數字的掌握來呈現，營運規則的更迭也反映在不同的應用系統程式的邏輯修改管理決策報表，因此原有的的風險控管目標雖然不變，但是控制實施方法，與稽核的能力，則出現了相當仰賴資訊技術的變異，主要的改變如下：

1.新資訊科技所可能帶來資訊安全課題，如分散式處理環境下複雜網路安全及安全管理之問題。

2.組織架構與職能分工轉變為應用系統角色及權限之扮演。

3.作業流程的調整與改變。

4.內部控制架構需轉化加入系統控制考量。

5.交易量增加及審計軌跡的消失, 增加控制及稽核上須進行變革。

風險管理包含指標，其中與資訊安全直接相關的課題是資訊處理與資訊技術之風險（information processing and technology risk），分述如下：

（一）資訊基礎架構風險（infrastructure risk）

此風險因企業組織未能建構完善的資訊科技基礎架構（如硬體、網路、軟體、人員及流程），在有效率及控制良好的模式下，支援企業組織現有或未來的需求。這些風險在於界定、開發、維護、經營資訊處理環境（如電腦軟體、軟體系統、網路等）的程序及相關營運應用系統（例如客戶服務、應付帳款、生產排程、信用處理）有關。舉凡從作業系統平台，資料庫系統，網路系統，實體環境等等，特別是現今 e 化環境對網路的依賴性非常高，因此資訊基礎建設之完備，傳輸之保全是重要的風險控制點。

（二）資訊可取得風險（availability risk）

當需要資訊執行營運決策或經營活動時，無法即時取得的風險包括因資訊通訊中斷所產生的損失、喪失處理資訊的基本能力、操作上的困難等；而企業營運的中斷也可以來自於天然災害、惡意破壞、怠工，甚至車禍等。資訊取得風險應著重以下三個不同層面：

1.藉由監督效能及在問題發生前採取預防措施, 可避免此風險。

2.系統臨時中斷的風險，可使用系統或資料回復技術使損失降至最低。

3. 因天然災害而造成長時間之中斷所產生的風險, 可透過應變計畫(disaster recovery plan 或 incident handling process)使資訊系統減少損失。

Arthur Andersen 與英國經濟學人雜誌發展出一系列企業營運風險管理架構(參見圖 5-4), 此項架構中關於資訊技術與資訊

處理之風險包括下列幾項：

圖 5- 4 企業營運風險管理架構

資料來源：Arthur Andersen Knowledge Space

（三）真確風險（integrity risk）

此風險會發生在資訊處理的兩個範疇，分別是資訊基本架構的管理、及維持組織營運所必需的應用系統。其風險在於資料的處理(manipulating)、擁有(responsibilities)、展現 (disclosure)

均違反了企業營運控制的實務、或資訊系統之輸出、入與處理的正確原則端控制程，如:資料轉換介面出錯、資料內容遭破壞，網頁內容遭惡意竄改、網路資料劫奪 (session hijacking) 及資料結算之錯誤或根本的程式邏輯與經營流程不相符。另一類型則如使用者權限的不相符或是系統導入之變更，傳統之部門間職能分工轉變為應用系統角色及權限之扮演，例如員工兼具請購人員與採購人員之權限，可能導致不當授權，將導致使用者存取未經授權之資料之風險，或造成機密資料外洩及未經授權之異動可能性。

（四）存取風險 (access risk)

資訊存取風險著重於不適當的存取資訊系統、資料和資訊之風險，它包括不適當的權責劃分、資料與資料庫整合之風險、以及與資訊機密性相關之風險。包括資訊、資料及程式存取被不適當核准或拒絕。不適當的人可能取得機密資訊，而適當的人卻被拒絕存取。資訊存取的風險是全面性的，亦即包括因任何目的而取得的資訊。

（五）攸關風險（relevance risk）

攸關性風險係指該資訊與蒐集、維護與傳達資訊之目的無關，該風險係與資訊系統所產生或彙總資訊之有用性與時效性有關。依性質而言，資訊的攸關性風險直接與「決策資訊風險」有關。此風險係指無法將「正確」之資料或資訊，傳達給「正確」的經營、消費或管理決策、決策程序、決策系統，在「正確」的時間內做出「正確」之決策。此風險之發生主要係因未充分了解資訊需求及缺乏對時效性的注意，進而妨害到交易雙方的權益、企業競爭的優勢或是管理的效益與效率之上。

當然，除了資訊相關的風險外，其他如環境面的法律風險、營運面的效能差異風險、授權不當風險均會直接間接衝擊企業的資訊安全架構。另外，針對不同交易個體間近來盛行的委外業務，如 ISP、ASP、IDC 等等，身為使用者的企業應確認

服務供應單位各項措施是否提供了系統安全或資訊安全，除了防範外部破壞，是否亦顧及了發生率最高的內部未經授權存取以及可提供的服務等級。

近年來由於網際網路的盛行及其存取能力的增進，以致 ERP 進入另一個新的領域。ERP 不僅是以往對企業資源的整合，且現可與電子商務合作對象做進一步資源結合。重要關鍵是導入以瀏覽器為使用者介面的 ERP 系統。這可使使用者無論在何處均可藉由網際網路進入 ERP 系統。例如：在外地的銷售人員或客戶可查詢訂單或存貨的狀況，供應商可查知之前貨運的情形等。

若由傳統的 ERP 改變為這種網際網路基礎的 ERP 系統，固然提供電子商務更寬廣且無時間限制存取資訊的效果，並能擴及至客戶及供應商。但其轉換尚有一定的風險性存在。內部稽核需瞭解且需參與其規劃，才能知道風險的所在及將控制點置於適當的位置。對於內部稽核來說是一個大的挑戰，一方面需不斷的充實攸關風險的知識，另一面需與專案人員密切合作，才能訂定出風險及知道如何管理新興的風險。

而在操作上的風險亦可能發生，如電子商店無法確認每一個使用者所用的電腦上安裝的瀏覽器是相同版本，其資料更新作業會因不同的瀏覽器或版本不一有無法完成情形發生。所以在網際網路基礎的 ERP 系統中設計有效的控制，確保使用者執行日常的工作能確實的完成是非常重要的。另一個需考慮的是系統的效能，因網際網路基礎的 ERP 系統，會增加軟硬體設施及網路架構的更改，則對於使用的硬體、資料庫及應用系統的規格與效能要有相關的控管風險。除此之外，更有下列衝擊造成電子商務之風險：

1. 各內部控制點往外延伸，與其他之控制點連動增加，導致控制複雜度
2. 與客戶及供應商之營運關係改變

3. 網路化安全之衝擊

4. 網路化系統之可信賴程度與真確性

5. 營運支援業務 (line of management) 的作業方式改變

6. 透過網路進行金流轉換之機制

7. e 化作業各系統間之銜接

8. 資訊技術之基礎架構未能配合營運需要

9. 技術與營運目標未能配合

10. 新系統導入但營運流程會隨之變更

11. 銷售資料與稅務資料的配合度

根據 2001 年美國 FBI 與 CSI 化（computer security institute）最新電腦舞弊與安全報告，有 70%之舞弊或失控來源點為網際網路連線（2000 年時為 59%），18%之攻擊來源點為遠端數據機撥接連線（較 2000 年時低）。這種引起管控失效的根源，已經不侷限於內部的作業流程與人為之缺失，包含外部惡意的破壞者，可藉由種種技術上的漏洞或電子商務內營運流程的轉接點（例如：兩個系統間之檔案傳輸，系統傳輸時之資料竊取與竄改），來破壞電子商務之資產或財務。

有鑑與此，導入資訊確認（information assurance）的控管機制對 e 化電子商務而言亦形重要，傳統針對電腦稽核的要求，僅限於資訊作業本身的一般控制與應用控制，針對電子商務所處之經營環境、資訊處理的過程、資訊來源以及處理結果對電子商務營運的影響均極少，僅藉著對稽核軌跡的確認，亦無法證明資料處理過程的完整與合理。

建置資訊安全系統都會關聯到成本。而風險造或損害時，至少會有更換或維護資源的成本，所以利用風險管理的方法，來分析資訊安全威脅是一種可行的方法。歸納幾個分析項目如下：

1. 經營需求：

包含在經營體系下會影響資訊系統的安全部份，如業務成長需求、對外的策略聯盟及業務不斷改變等。

2. 一般設備：

包含房子、空調、佈置、或其他支援資訊系統的設備。

3. 資訊設備：

包含主機、工作站、電腦、網路設備、紙張、磁碟、磁帶等，與執行資訊系統有關的設備。

4. 軟體：

包含購買的或自行開發的商用軟體。

5. 資料與資訊：

定義在電腦、網路上的資料或資訊儲存與取用。

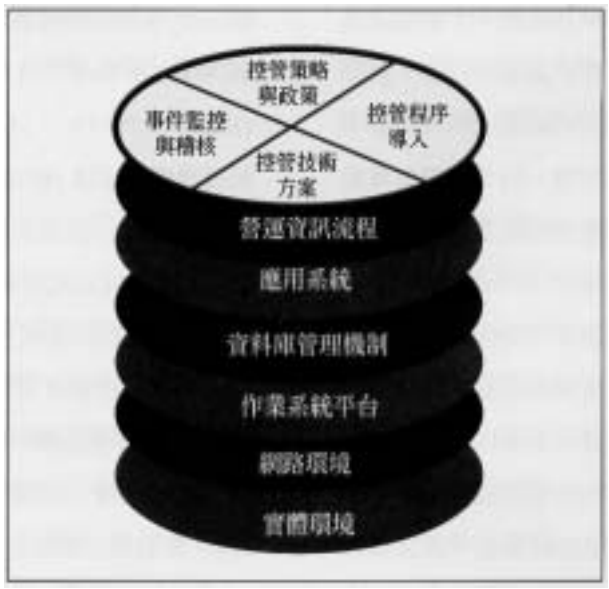
6. 個人：

泛指與資訊有關的企業員工、協力廠商員工，或外在使用資訊系統的顧客。

有鑑於此，電子商務資訊確認之控管築構，期望藉由對電子商務營運目標的了解，以及決策之重要性，來了解資訊處理過程可信賴的程度，而非僅僅對資訊安全之問題解決。藉由此項過程將 e 化環境的控制與營運流程及經營目標結合，以分析資訊的可確認程度(information assurance)，其架構如圖 5-5：

藉由此六層四個向度之架構，來切分各類網路化系統的組成成分，並利用典範實務資料庫，提供各類流程的最佳實例，供各類產業與電子商務描摹其作業與資訊處理之關聯，藉由此種關聯可以定義出資訊作業之自動化部分、人工化部分、控管點，以及各營運流程控制之情形。

圖 5- 5 六層四個向度之架構



資料來源：參考書籍 R2（十三）

圖 5- 6 應用系統與流程之整合

Task Group Description	Grp	1	2	3	4	5a	5b	5c	8	9	10	11	12	13	14	15
		AP Voucher Entry	AP Payments	AP Release Blocked Inv	AP Clear Vendor Acct.	Vendor Mast. Maint. FI	Vendor Mast. Maint. MM	Vendor Mast. Maint. CEN	Bank Reconciliation	AR Cash Application	AR Clear Customer Acct.	Material Master Maint.	Service Master Maint.	Requisitioning	Release Requisition	Purchase Order Entry
AP Voucher Entry	1		X	X	X	X	X	X								X
AP Payments	2	X				X	X	X	X							X
AP Release Blocked Inv	3	X														X
AP Clear Vendor Acct.	4	X														X
Vendor Mast. Maint. FI	5	X	X				X									X
Vendor Mast. Maint. MM	6	X	X			X										X
Vendor Mast. Maint. CEN	7	X	X													X
Bank Reconciliation	8		X							X						
AR Cash Application	9								X							
AR Clear Customer Acct.	10															
Material Master Maint.	11													X		X
Service Master Maint.	12													X		X

資料來源：參考書籍 R2（十三）

其控制之良善，以政策/管理程序/控管技術/監督與稽核等向度來分析可能造成的風險。針對應用系統與流程之整合，可採用 SAP MM Module 主檔新增、修改流程之完整性為例說明(如圖 5-6)：

1. 風險與控制

（1）無全部主檔資料之新增、修改皆已在系統內處理。

（2）主檔資料之新增、修改輸入不完整。

（3）主檔資料之新增、修改重複輸入。

2. 系統控制（欄位狀態）

（1）欄位設定模式：

- Hide (隱藏)
- Display (顯示)
- Reqd. entry (須輸入)
- Opt.Entry (可不輸入)

（2）當執行物料主檔維護作業時，有部份之欄位必須輸入資料才能儲存時，其欄位會以「?」顯示。建議於執行物料主檔維護新增作業時，下列主檔欄位應設定為強制輸入：

- Order Unit
- Material Group
- Material Type
- Automatic PO
- Source List
- Purchasing Group
- MM/PP Status
- Purchasing Value Key

(收貨無上限的欄位應不設定)

- Quality Inspection

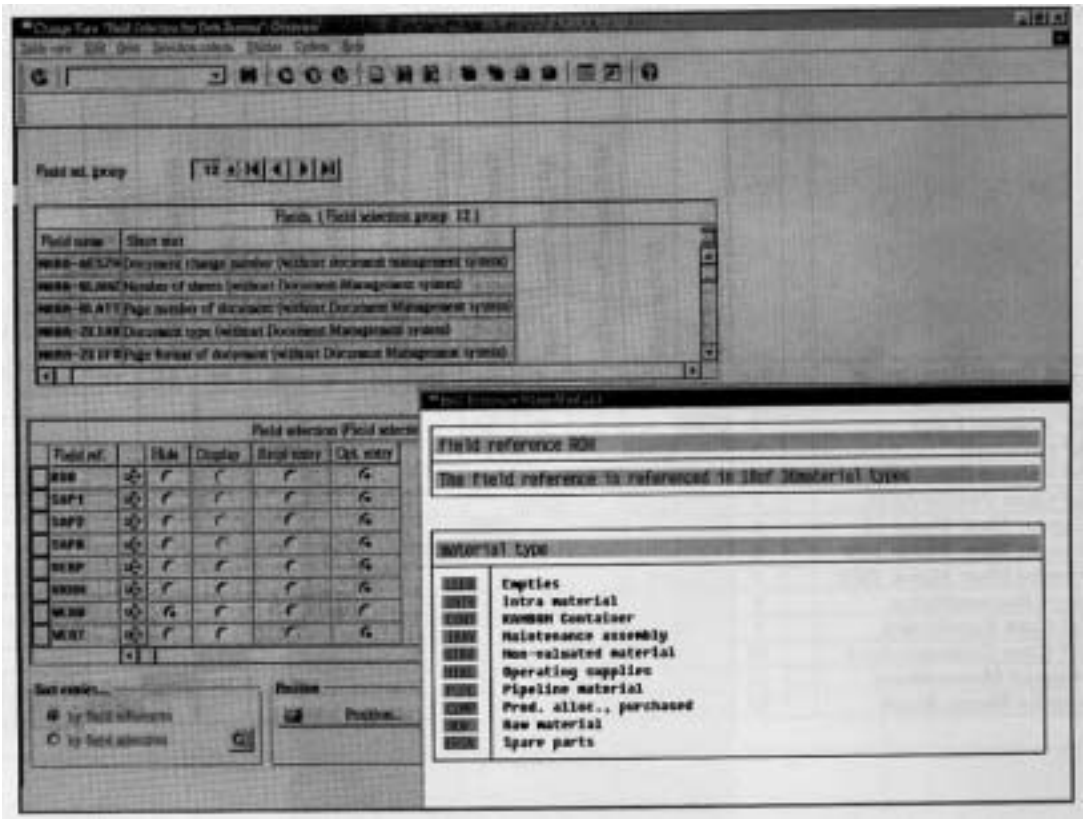
(有使用 QM 模組時)

(3) 測試方式 (範例)：

執行路徑：SPRO→IMG → Logistics-General→ Material Master → Field Selection→ Maintain Field Selection for Data Screens

(4) 畫面範例：

圖 5- 7 風險控制測試畫面範例



資料來源：參考書籍 R2（十三）

（5）設定目的:

選擇重要欄位確認其設定為「Reqdentry」，以確保重要資料於執行作業時確實輸入。

而於其他階層，如於應用系統層則包含為便於決策或資訊處理之企業營運資訊系統，例如 ERRSCM 以及網站系統等，其中各項系統均有其特別之控管內涵與技術設定的結合之處，例如 SAP 系統，其權限之表達高度仰賴於 SAP 的授權物件(authorization profile)，電子商務依控管實務，搭配 SAP 專家，開發出權限衝突矩陣，藉由風險顧問進行差異分析(gap analysis)，可以將目前影響作業真確性的系統/作業邏輯點出。針對其它階層，如：

甲、資料管理層 (data layer)

包含利於資料擷取與使用之儲存相關技術環境，如資料庫管理系統，其使用權限、系統安全、資料庫控管等之控制，以及資料庫設計時之合理性與技術可信賴程度，目的在確認資料的儲存與讀取之真確性，因此資料模型之設計與分析，為相當重要之重點。例如資料邏輯模性之正規化以及邏輯模型與實體模型之對映。

乙、系統與平台層 (platform layer)

包括儲存/處理資訊與交易所在之系統硬體與作業系統軟體。

丙、網路層 (network layer)

包含提供系統相互聯結及通訊相關之資訊技術，例如:區域網路/網際網路/撥接服務/路由與連線設備等。特別是網路風險包含擷取設備、網路認證機制、網路系統開發元件、開發技術等均影響網路於資訊傳遞之隱私性與真確性。

丁、實體層 (physical layer)

包含所有資訊處理設備及所在環境之實體控制，例如機房/設備/網路元件/佈線/門禁，防水/防火/溫控/進入路徑，結構與佈建，備援方案以及事件處理機制 (incident handling)。

經由此種方法來控管 e 化風險，優點在於降低稽核之複雜程度，並易於妥善處理各階層之關聯性，以及將營運目標與資訊技術之控制結合為一體，方能使稽核之作業控制之效果獲致績效，而非僅針對技術之安全分析，使得企業進入 e 化時代遊刃有餘。

二、風險辨認---辨認哪些資訊系統具威脅性

非資訊科技背景之企業主或主管一定被最近一堆 eBusiness、Internet、eCommerce、駭客入侵…等新世紀電腦名詞搞得神魂顛倒，想使用新資訊科技輔助企業營運，但又害怕不知如何指揮資訊人員或掌控資訊風險。

不論任何作業或營運絕對不能只以「人」來管理，資訊科技更是如此；因為人有七情六慾，每個人的作風要求均不相同，恐因人員替換而影響資訊系統運作、管理及安全。同時，e 化環境下，亦非只要有一套「防火牆」設備即可高枕無憂，需具備完整之配套措施，讓入侵破壞者無一絲空隙可進入。最佳方法乃規劃一套適合各家公司實際營運狀況之 「資訊安全管理」制度，透過程序化方式管理公司資訊系統，讓專業資訊人員明瞭如何依據規範管理資訊系統，且主管亦能掌控全貌及風險。如何規劃一套合適之「資訊安全管理」制度呢？想必又是另一難題。

一般而言，企業應有專責單位負責執行資訊安全風險評估，該單位協助企業內成員評估各項資訊風險等級。一般企業會將資訊分成三種等級，一是公開資訊、二是提供客戶或供應商所使用的資訊、三是內部所使用的資訊；企業可依需求作適當的調整，如自行規劃為高風險性資訊、中風險性資訊及低風險性資訊三種等級。然而由各種實務來看，資訊安全政策的制定都是完成整體資訊安全政策，可作為資訊安全政策制定的參考。

資訊安全系統的風險來自外在威脅及自身弱點。威脅及弱點會損及資訊資源、系統及網路的可使用性（availability)、完整性（integrity）或保密性（Confidentiality)，造成系統降級。所以對每個資訊資源或事件的威脅或弱點，都須個別評估一旦發生時所

可能造成的損失，包括資訊系統替換或維修的成本；將資訊系統重建為具智慧資產的成本;資訊系統停擺所損失的價值；以及其他（如顧客或協力廠商失去信心）。

兩種資訊安全的迷思：第一是資訊安全產品本身的使用不能代表任何安全防護效果，必須搭配適當的裝設、設定管理（configuration management)、系統管理與監控稽核。第二則是單憑某一項資訊安全技術的使用，很難達到安全保護的效果，因為資訊安全的評估需要保密性、真實性與可運作性三者同時考量。

圖 5- 8 資訊資產之安全性

資料來源：Emst & Young

所以說，風險評估分析是針對資訊資產之安全性進行定義的過程，植基於下列三種資訊的特性：機密性、完整性、可用性，如圖 5－8 示意, 同時涵蓋針對資訊安全做法上如何確保所有資訊資產都被適當辨別、證明及維護的控制方法。風險分析的主要目的是辨認及分析資訊資產的相關風險，並決定適當的保護措施及控制方法，以減低風險層級及其可能之影響。

（1）機密性：例如薪資資料、研發單位的成果等。

（2）完整性：資訊是否完整？是否被竄改等。

（3）可用性：當要使用資訊時，該系統是否可以適時地提供服務等。

然而導入資訊安全管理之專業經驗，下列提供下以步驟供進行規劃符合上述三大目標之資訊安全管理制度：

步驟一：定義範圍 (scope)

首先需定義此次資訊安全管理所欲規劃之範圍。例如: 公司、廠、或某一系統作業等，依據實際需求定義一個合適之範圍。若公司專案規劃小組係第一次進行規劃此種制度，則最好選擇小範圍、相關人員易配合或較易於導入之部分列為優先範圍，以免初期失敗造成信心大減。

步驟二：資訊安全剖析階段 (security profiling)

針對步驟一定義之範圍，盤點該範圍之資訊資產，同時進行以下主要分析評估程序：

＊ 威脅與弱點分析：

依據各種資訊資產分析其可能具備之威脅與弱點；另外，有關資訊技術之相關漏洞或弱點，則應指定專人負責收集或委外予顧問協助提供資訊，避免遺漏重要資料而疏於規劃適當避險措施。

＊ 評估資訊系統基礎架構：

針對現行公司之資訊基礎架構進行初步評估程序，例如防火牆、作業系統、資料庫或遠端存取系統等之控管方法。該等控制管理方法應不僅止於系統技術面之考量，更應包括管理程序面。

＊ 意外事件通報流程：

評估意外事件發生之檢核、評估影響等級及通報程序是如何進行，能否有效且及時處理意外事件，減少公司損失。

步驟三：資訊安全架構階段 (security architecture)

依據前一階段所找出相關資訊，開始設計以下規範：

＊ 制定資訊安全政策：

依據分析評估資訊，著手撰寫書面資訊安全政策，作為安全管理之最高指導原則。

＊ 技術分析：

包括資訊資產等級分類及搭配相關資訊技術之運用與管理。

＊ 風險評估/控制管理程序：

為下一個架構規劃程序鋪路，則需進行一次風險評估及控管程序之規劃工作。

＊ 組織架構規劃：

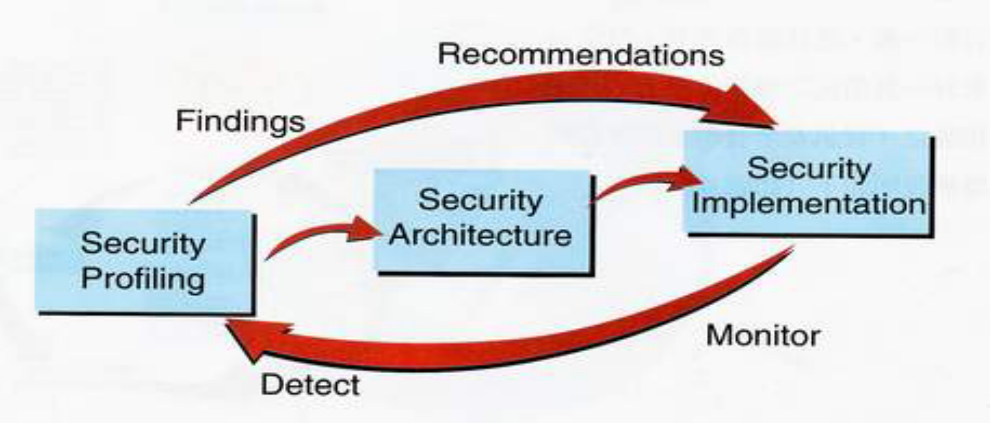
依據上述資料，彙總規劃一套合適之資訊安全管理架構藍圖。

步驟四：資訊安全導入階段 (security implementation)

導入上述資訊安全管理架構之解決方案，包括遠端存取安全、防火牆、加解密等技術與管理方案。

上述步驟二至四乃為週期循環，經由不定期巡迴覆核及修正成企業體最適切之資訊安全管理制度，圖 5-9 為資訊安全管理架構圖。

圖 5- 9 資訊安全管理架構



資料來源：Emst & Young

建置一套資訊安全管理制度看似容易，若無實際經驗執行起來恐怕頗為困難。尤其欲憑空想像規劃一套制度實為不易，不如參考現成規範或標準，再來量身訂製一套，應該較為容易。目前台灣國內尚未有一套類似之標準供參考，而國外則早有相關之「資訊安全管理」制度規範可參閱，舉例說明如下：

1. BS7799：-

係英國所制定有關資訊安全管理之標準，目前該標準之 Part l 部份已經成為 ISO 國際標準 (ISO17799)，其可分為 10 大項目、32 個控制目標及 127 個控制程序;該 10 大項目包括：資訊安全政策、資訊安全基礎架構、資產分類與控管、人身安全、實體與環境安全、通訊與作業管理、存取控管、系統開發與維護、企業持續營運管理。

2. COBIT：

國際電腦稽核協會 (ISACA)組合專業團隊 (來自產、官、學代表)依據實務經驗，針對資訊系統控管所制定之控制目標、執行與稽核程序。其主要分為四大主題：規劃與組織、取得與建置、交付與

支援、監控。其中更包括 34 個主要控制目標與 302 項控制程序，係一份極為詳盡之參考文件（圖 5-10)。

圖 5- 10 資訊系統控管

資料來源：COBIT

3. 資訊技術面參考文獻：

另外與資訊科技較為有關之參考資料包括 NIST、ISO15408 及 ISO15504 等，其為針對產品系統或處理程序等相關之資訊安全規範。藉由上述等參考資料協助專案團隊順利規劃一套資訊安全管理制度，供相關人員遵循。

如此一來，企業主或高階主管只要定期監控該程序是否落實執行，即可將資訊風險 e 把罩。非科班出身之主管可藉助電腦稽核、認證或委外予專業資訊安全稽核顧問，協助檢核是否依序執行，同時亦可提供更為客觀之第三者建議予公司，更能做一次流程修改之機會，提升安全與執行績效。

綜合「風險評估對象」所提出的評估對象，再細剖析各個可能產生的威脅或弱點。

（一）經營需求：

根據經營需求，可在業務成長、企業策略聯盟及業務不斷的改變等三個需求方面，從事資訊安全與資訊政策的威脅考量。

（二）一般設備：

這些設備可能面臨的威脅來自火災、水災、地震、炸彈及一些化學藥品的污染等。這些威脅發生時會癱瘓資訊中心，繼而造成停工的損失成本，或重建及測試的成本。

（三）資訊設備

資訊設備可能面臨火災、地震及人員安全管制不力的威脅。最重要是，資訊設備不能被未經許可者使用。

（四）軟體

程式遭使用者或程式設計師意外修改或破壞、被不安全程式影響而當機，利用備份資料時不正當使用資料、裝設新軟體或修改後的軟體採用了不安全的新程式碼，這些都是使用軟體

所面臨的威脅。

（五）資料與資訊

儲存媒體是否安全、網路資料受到駭客攻擊、受到遠端不安全的網路資料取用、檔案被偷或遭破壞，都是使用資料所面臨的威脅。

（六）個人

競爭敵手指使員工偷竊資料、不滿離職員工報復、或為私利複製資料、協力廠商員工利用電腦使用權限偷竊資料。員工是否盡職管理系統？是否讓網路繼續正常執行？是否降低資料被盜用的可能性？都是個人威脅的考量範圍。

（七）其他必須考量的風險

欺騙與偷竊（如假冒權限盜取財務系統、庫存系統及薪資系統資訊等）、惡意的駭客攻擊、商業間諜盜取資料行為、電腦病毒的感染及如何保護個人隱私權等。在考量威脅時，企業並不須逐項考量；只須衡量自身情況找出主要威脅，再估算可能的損失與防範之道。

國內證期會針對公開發行、上市及上櫃公司訂定內部控制實施要點中，對企業設置資訊管理控管的十項要點，或是行政院研考會針對行政院所屬各機關對於資訊安全的執行要點，對比英國標準組織的 BS7799 或 ISO17799 資訊安全管理系統實務準則，其大要並無差異。因此雖然資訊安全政策的內涵相似度很高，但由於企業的經營特性、資訊技術環境等特質的不同都會影響資訊安全管理程序上的差別。為了量身訂製符合營運實務的資訊安全管理體系，各類組織要如何來進行資訊安全的導入呢？試參考 BS7799/ISO17799 的資訊安全導入流程，如下圖 5-11 所示。

圖 5- 11 BS7799/ISO17799 資訊安全導入流程

資料來源：參考書籍 R2（十二）

整個資訊安全對於企業而言，最大的意義是風險管理，而非僅是系統的保全。因此品質確保與不斷地評估修正、善用專業稽核來確保資訊安全管理體制的落實執行為目前之世界潮流，亦有越來越多與歐美先進國家進行交易時，要求交易方提供足夠的資訊安全保證，以確保資訊資產之交換不受到戕害。

美國政府對於牽涉到公信力和需要外部稽核以保證資訊安全控管作業品質的營運時，許多任務均要求具備專業執照的專家出任，以華盛頓州、猶他州與明尼蘇達洲為例，要求 CA 業務經營業者需經過外界公正單位的資訊安全與控管之稽核，稽核單位可由個人或團隊方式執行，其條件是為具備會計師資格（certified pubic accountant）與電腦安全專家資格，其中電腦專家資格可為國際電腦稽核協會所認證之電腦稽核師資格（CISA），或是國際資訊系統安全認證組織所認證之資訊系統安全專家（CISSP），無非是期望有一公正第三者，以國際可接受之規範，對資訊安全與風險控管進行具品質且中立之評估。企業應該將每項資訊資產作量化價值或風險等級評估，再依據評估結果作適當的保護措施，因為資訊安全的重要觀念是：使用適當成本來保護我們的資訊資產。

三、風險估計---估計威脅所產生的損失

風險評估被認為是評估資訊系統安全的重要步驟，以引導出資訊安全之警覺性，進而提供適當機制來衡量風險大小，並協助評估及選擇適當的安全措施。風險評估不是一段時間的工作，而是隨著科技及企業變化而持續改善的過程。

對於每個系統或邏輯資料的存取，建議資訊安全專責單位協助企業的資訊擁有者或熟悉資訊資產的人員進行下列分析：

（一）評估資訊資產之重要性，並考量下列因素：

（1）資料是否需要高度機密性或財產化。

（2）資料是否需要高度完整性及一致性。

（3）資料是否常常被使用。

（4）稽核所有作業的潛在威脅，已決定各種風險發生之可能性。

（5）利用適當的資訊安全政策及標準，定義出使用者如何適當使用資料的方法。

資訊系統的威脅產生時，必須先估算可能的損失，才能提出防範之道。對每一風險項目設定風險產生的年出現率（annual frequency rate），事先評估威脅出現的機率，接著再設定每年可能產生的損失期望值，而「損失期望值=每次損失*出現頻率」。風險產生的年出現率設定方式如下：

100 年出現一次	(. 001)
10 年出現一次	(. 01)
3 年出現一次	(. 3)
1 年出現一次	(1)
100 天出現一次	(3)
10 天出現一次	(30)

1 天出現一次 (300)

1 天出現 10 次或 100 次 (3000)

損失期望值的計算應結合「風險評估對象」及「風險辨認」中的各評估項目，再參考下列威脅產生的途徑，找尋各個項目的威脅估算損失值。

（1）從自然環境的威脅：

如水災、火災、颱風及地震等。

（2）從人員的威脅：

人員操作錯誤、系統程式錯誤及電腦當機時間等。

（3）從建造環境的威脅：

電腦硬體損壞風險接受的標準。

（4）成本/利益的考量：

保固資源的花費不會超過威脅所造成的損壞。

（5）生活中風險可能產生的影響：

我們總是生活在風險中，應記錄各種風險的產生是否與成本相關，做為下次風險評估的依據。

在「風險估計」中，先找出主要威脅及弱點的每年損失期望值，接著估算防範建議的成本，在成本與經營需求間，找出企業可容忍的風險範圍，進行資訊安全設備與技術的投資。

而風險評估經由一連串嚴謹的過程，將每項資訊資產作量化價值或風險等級評估，以下我們分為十一個步驟加以說明。

1. 決定評估之初步範圍

風險評估的第一步先要明確了解企業的業務領域與工作性質，決定哪些資料需要被防護之前，必須要了解這些資料對企業的重要程度，在來定義風險評估範圍，最初的風險評估可能會侷限於

某個範圍內，但所有的資訊資產在最後還是會被評估到。

2. 企業單位之分類

將企業各單位依編制及功能進行分類，並且和各單位的高階主管進行訪談，由各單位高階主管決定單位內哪些人員應參與風險評估之規劃。

3. 召集風險評估專案團隊

風險評估規劃必須要與企業資訊安全體制相互協調，企業需由下列個別領域人員來組成專案團隊：

（1）高階主管

（2）資訊中心人員，包括資料處理操作管理員、系統管理員、系統分析人員、程式設計人員、網管人員

（3）稽核單位

（4）法務單位

（5）應用系統使用者代表

風險評估專案團隊主要人員，應該由企業各單位高階主管及各應用系統使用者代表構成，對整個企業運作與資訊系統了解的幕僚人員亦應支援該團隊。資訊中心人員是經授權的資訊管理者，而非擁有者，因此，他們對於資料本身的權利及責任是有限的，所以資訊人員應該在團隊運作時扮演技術顧問的角色，而資料存取控制及資料評估則是資訊擁有者的責任。

4. 技術系統及平台分類

將技術、系統及平台做明確定義及適當分類。

5. 辨認目前所使用軟體

完成上述定義與分類後所有的技術、系統和平台，即可列出一份應用軟體明細表。

6. 辨認資訊擁有者

當確認企業之應用系統並記錄後，資訊擁有者須加以辨認，並重新評估，此步驟之重點在於辨認和資訊的收集;風險評估應從企業整體運作層面開始著手，並定義分類資料的邏輯。風險評估專案團隊成員以小組的方式進行，每個小組針對各個應用系統搜集相關資料，其工作內容為：

（1）決定資料重要性(非常重要或不重要)。

（2）決定資料機密性(半公開資料、內部資料或公開資料)。

（3）針對每種資料，決定資料特性(可用性、機密性、完整性)。

（4）評估資料安全受威脅時，會對企業造成的影響及損失。列出可能發生的風險、弱點與威脅。

在初步審核過程後，專案小組應該一起評估產出結果;因為每個成員對企業需求有不同的認知，因此所作資料分級較無法客觀，故需透過公開的相互討論，並就討論結果作適當修改，以達到資料安全等級分類、可能產生的風險與資料價值範圍。

7. 企業整體風險評估

目標是評估之前步驟定義的資料所可能面臨的風險，並由專案小組評估該風險對企業會造成的影響，其工作包括：

（1）審核所定義的風險並決定其可能發生機率。

（2）定義風險可以被接受的程度。

（3）從企業運作的風險角度，評定資料等級。

8. 訂定可接受的風險等級

風險分析時，對於任何控管風險的花費都不應超過該風險產生的最大損失。要達成具經濟效益的資訊安全解決方案，風險分析需要確認企業的 可能損失，或是各個項目的價值異動。確認風險及攸關損失後，並無法決 定哪些風險值得採取行動，一旦損失估計出來，再繼續下列執行步驟：

（1）確認企業可忍受風險之大小。

（2）針對各項風險之投保策略。

（3）減少損失之防護措施費用，或是降低風險發生機率之防護措施費用。

資料保護的方法包括相關資訊安全產品、安全政策與執行程序之落實，在資訊生命週期的每一個階段，資料均應受到安全防護，儘管資料的狀態已經改變，但資料重要等級必須維持不變(例如:資料已列印為報表格式、或儲存於磁碟機內、或已口頭論述)，在執行時需考量員工行為或人機介面的安全政策或程序是否已被適當保護，因為完整的資訊安全政策不能有空窗期。

依據企業各單位業務特性，確認可承受風險程度之後，風險評估專案團隊需重新將這些資料加以分類及排列順序，以確保機密性之資料已經過辨識並且確認其安全等級高低。

9. 資訊存取的管制

資訊重要性等級分類排序後，須進行蒐集電腦系統與應用程式相關資訊，以協助資訊擁有者落實資訊分類的控管。

10. 安全政策擬訂

風險評估的分析結果須由行政、技術與程式管理者相互稽核、確認及執行，最後再藉由資訊擁有者對於安全政策的資訊分類，規劃執行並對程序做最後確認，例如各部門電子與書面資料的傳送須符合流程，並適當規範資訊擁有者在傳送過程所扮演的角色。另外，安全政策與標準必須符合企業預算、取得員工接受、滿足企業發展前景、在技術上是可行的一套安全標準。

11. 內外部系統風險再評估

當前述工作完成後，企業應持續執行相關管控措施，在整體安全管控要求下，以期達到符合企業需求的資訊安全政策;此外，資訊擁有者須定期檢視資料分類計劃與執行狀況，確保資訊安全

分類之有效性。

對於風險評估及撰擬資訊安全政策階段，除依風險評估結果做為辨認風險因素之適當控管政策外，並應由負責評估及考核政策安全性的單位執行持續稽核的程序，以確保資訊安全政策建置的有效性及完整性。

四、風險控制策略

沒有百分之百絕對安全的資訊保全措施。既然風險沒辦法全部移除，就必須管理。有效的風險管理即是將資訊安全合格化、有效量化風險因子，並減低其發生的可能性。針對「風險控制策略」，應擬定一套有效、適用的資訊安全政策，符合企業經營需求、資訊設備、軟體、資料、資訊與個人等項目的風險控制要求。主要執行重點歸納如下：

（一）定義資訊安全範圍

從「風險評估對象」至「風險估計」的各項風險因子分析，資訊系統安全範圍應涵蓋各項資訊資源及介面使用所需考慮的範圍。各項途徑的破壞都會產生損失或不便，且網路也要有保密性、完整性、可使用性及不可否認性的機制。所以資訊安全範圍包含下列系統項目及資訊安全設備與技術：

1. 設備：

保險、保全系統、門禁系統、安全監視系統、自動灑水系統。

2. 網際網路安全：

防火牆考量、資料傳輸安全控制、VPN/EDI（如病毒防制、入侵偵測、安全稽核、備源系統、備份/恢復）。

3. 使用者安全：

使用者管理/群組管理、身分認證、單一簽入驗證（如

存取控制、使用授權、資料加解密、網路儲存記憶體、備份/恢復)。

（二）進行資訊安全的整合規劃

以「風險估計」防範安全成本考量，企業資訊安全是一種投資。應先有策略性規劃，且要兼具經營導向、成本/利益分析的思維及法律與規章的設計。整合規劃應涵蓋策略、執行、量度與稽核的控制。

（三）擬定資訊安全政策

擬定企業資訊安全政策之前，應考量的因素如下：目標要能影響行為、方案要能被執行而不是被拒絕、安全措施容易施行、當成銷售成本而不是負擔、確定企業哪些資料必須處理、如何存取、哪些是組織中最重要資料、資料需要何種控制。茲歸納成兩點說明如下：

1. 撰寫資訊安全政策應符合：

（1）符合單位文化

（2）使用真實的資訊管道

（3）應包括法律、人力資源及公開的職務

（4）資訊安全政策是單位最高指導原則

2. 資訊安全的熟知與訓練應考量：

（1）設計資訊安全標準的處理程序

（2）新進人員需要資訊安全的受訓

（3）每年簽署安全條文

（4）以網路新聞方式加強資訊安全的公布，或有線上版的資訊安全條文。在擬定資訊安全政策時，可參考行政院研考會為各級政府機關規劃之「行政院及所屬各機關資訊安全管理規範」。（網址：

http://www.rdec.gov.tw/eno/security/）

（四）規劃資料與資訊的分類

與營運相關的資料或資訊，是企業相當重要的資產。除擬定資訊安全政策，另一要項即規劃資料與資訊的分類。首先依據資料的性質可分為：個人客戶資料（如財務資料及訂單）、經營單位競爭資料（如財務資料、商業資訊及競爭者資訊等）、員工資料（如薪資、個人隱私）三類。再來設定資料與資訊的建立、儲存及分送制度。針對資料與資訊取用的安全等級可分成：非限制性（員工、協力廠商都可取用）、限制性（限高階主管或特定主管）、限制分送（功能導向，因應業務需求而設定）三種方式。

（五）設計資料與資訊的取用

資料與資訊分類後，可把資料存放在個人電腦、檔案伺服器、公司內部網際網路主機或資料庫中。或存放於公司外部網際網路主機，透過區域網路、廣域網路，或經由網際網路的 http、ftp、email 傳送資料。當包括內部員工、外部員工、合作伙伴、個人客戶、協力廠商等各種使用者取用企業資料或資訊，須確認資料的安全等級及其使用權限。企業有價資料的取用權，要在安全等級規範的目標下完成。

五、建立風險管理表

建立的風險清單是風險管理作業的初步，不僅僅是電子商務作業規劃工具，並可幫助提昇整個組織對風險的認知與了解。

Allstate 保險電子商店內部電子商務人員發現，他們電子商店新建立的風險清單不僅僅是電子商務作業規劃之工具，並可幫助提昇整個組織對風險的認知與了解。

Allstate 保險電子商店內部稽核部門最近建立了一套電子商務風險表，這是電子商店在注重風險管理整個流程，以風險導向

為稽核方式來執行中非常重要的一步。電子商務相關主管認為電子商務風險表除可幫助管理作業達到部分稽核目標外，更重要的是，電子商務風險表可提供電子商店對於風險管理的支援，同時預期電子商務風險表將可以發揮下列之功能：

(1)辨認對電子商店其有重大妨礙的風險及確保上述風險於規劃過程中已列入考慮。

(2) 促進風險管理人員在稽核內部或與管理階層討論中，對風險有更多之討論。

(3)建立電子商店內部對風險變化之監控及立即辨認新風險產生之基本架構。

(4) 為管理階層及內部稽核對風險作預先的準備，而非等到風險已造成效率降低後才有所反應。

(5) 加強電子商務人員風險方面之專業知識，並了解那些風險對本電子商店具有威脅。

Allstate 在一位教授擔任顧問下，於 1998 年開始發展電子商務風險表，其所完成的報告，在 1999 年的稽核規劃中，成為一項既重要又非常有效的工具，我們已經將它建置成本電子商店之策略，以作為管理詭譎多變的風險之機制。

（一）建立風險表

本電子商店在顧問的整合及幫助之下發展風險表，其過程包含以下四步驟：

步驟一：辨認及定義重大風險

每一位小組領導人（都是資深稽核，對他們所負責稽核的部門或功能，具有深度的了解）都個別被要求撰寫 10 項，針對他們所負責稽核單位或功能所面臨具有威脅的風險，同時被要求對所提出的風險，以一個句子的長度下定義。區域

稽核主管則個別對其所負責地區，辨認並定義該地區所遭遇的風險。於發展個別的風險項目時，小組領導人及電子商務管理階層對於固有風險（inherent risks）觀念彼此交換意見，並對固有風險下定義為：如果沒有相關的內部控制，具有威脅電子商店單位或功能之風險；這項工作與我們的信念相符，亦即當我們對風險做評估時，是依其重大性與可能性去決定該風險是否重大到應加以管理。如果答案為是，則我們必須決定該風險應如何管理，同時評估經過控制後的剩餘風險 （residual risk）是否已達可接受的水準。如果就重大性與可能性而言，該風險並不具重要性，則我們需要確保電子商店沒有分配過度的資源去管理它。

步驟二：整理並歸類風險

之後，管理階層及小組領導人分為四組，各小組個別針對已被視為對本電子商店具威脅的風險開會討論，在各小組內經整理歸類彙整後，由各小組召集人將該小組共同決議之結果交回。接著，各小組召集人分別說明各小組為何認為該事項為風險之原因，並共同將所有的風險重新組織分為兩類，分別為內部風險及外部風險。當一組接著一組說明其認定為風險的原因時，各小組召集人同時進行分類之工作；最後，另外一工作小組將上述會議的結果再次的整理，並重新轉換為風險表草案。

步驟三：建立風險表草案

工作小組設立了明確的準則，以判斷是否將風險列入風險表草案（控制的缺失則不列入）。將風險分類完成後，再以現有的風險模型去檢驗風險表的妥當性與完整性。在此同時，工作小組也根據各小組所繳交的風險定義，發展成為風險辭典（Risk Glossary），並對電子商務風險定義為「對單位或功能的目的、目標或成功執行策略具威脅，此威脅包括了『不好的事項發生』及『好的事項不發生』」。

根據所完成的風險管理準則，工作小組以『將導致發生及將導致潛在不利的結果』的字眼，另對風險建立簡潔的定義，在這之中，若有涉及或暗示到缺失的字眼，均被刪除。

在電子商務風險表的發展過程中，風險辭典扮演著一個重要的構成要素。所有辭典裡的用詞均是以電子商店的目的、目標及策略內容為範疇。而風險辭典幫助電子商店對風險用字歸於一致與統一，同時加強了對過去可能被忽略或未發現的風險型態之了解。

到此，初步的電子商務風險表及風險辭典草案已完成，並呈遞給管理階層及小組領導人檢閱，檢閱後所有參與電子商務風險表發展過程的參與者，均被要求去檢視該文件。

步驟四：詳細討論風險表草案

經過所有參與者的討論、提供意見及建議，使得電子商務風險表及風險辭典得以更精緻，成為風險管理稽核規劃的主要參考工具。

（二）風險表與電子商務規劃

在作電子商務計劃的過程中，風險表及風險辭典在以下三方面有極大的幫助：(1)與管理階層溝通電子商務風險；(2)為個別單位及功能建立較特定的風險清單；(3)建立電子商務項目之優先性。

1. 與管理階層溝通電子商務風險

與管理階層的對話中，討論用以管理風險的方法，及這些管理方法對電子商務作業的影響，除了傳統的內部控制 制度外，另有一些風險管理技術，其中包括風險迴避、風險收納及風險移轉。在與管理階層的討論中，也明確的表達內部電子商務不可能對清單內所有的風險均予以稽核，特別是那些主要的管理方法，並非經由傳統的內部控制制度所管理的風險。

有些管理階層在其所負責的領域內, 已貢獻相當多的時間與努力去對風險作紀錄並下定義, 當在與這些管理者討論電子商務風險時, 將由風險導向之稽核觀點所產生的風險清單, 與管理者觀點所認定的風險作比較, 如此對風險的雙向交換意見, 使得對組織所面臨的風險有更進一步的認知。

2. 建立特定的風險清單

藉由與管理階層討論風險表與風險辭典, 為特定電子商務風險的紀錄與定義, 提供了一個非常好的起點。不僅力圖為電子商店單位與功能建立風險清單, 並力圖將它作為風險管理清單的一部份。對風險有一致的專業術語, 對於整個組織對電子商務風險的溝通將有助益。除此之外, 一致的專業術語將會幫助對於跨電子商店單位與功能間, 對具有全面威脅的風險評估作整合。

3. 建立電子商務項目之優先性

特定的風險清單, 對於在評估個別風險的重大性與可能性, 實在是非常有價值的工具, 經評定為最高度的風險（分為高度、中度、低度三級）時, 將它標示為『關鍵』風險。當將關鍵風險與經評定為對電子商店單位及功能具重要性的電子商務流程連結, 可歸納出以下兩類具有稽核優先性的分類：

（1）有多種風險威脅的關鍵電子商務流程。

（2）對多種電子商務流程具有威脅的風險。

前一類, 將稽核的優先性放在架構於特定電子商務流程中的所有控制；第二類, 將稽核的優先性放在架設延伸於多種流程的控制上。決定何種不必稽核就如同決定何種必須稽核一樣重要, 最後終於發展出一

套流程與風險的組合, 並將它分為計劃去電子商務與計劃不去電子商務兩組, 而這套組合提供了管理階層一項了解，並評估電子商務計劃的簡潔工具。

4. 電子商務風險表衝擊

利用電子商務風險表來規劃稽核流程, 一般稽核計劃並不會發生戲劇性的改變, 部分傳統上所執行的查核工作仍然是被執行著, 電子商務風險表加強並幫助了基本的稽核方式, 更加清楚的了解影響稽核計劃的所有因素, 跨及本電子商店所面臨的所有風險，並加強了對所有高風險之了解。

經由電子商務風險表的發展過程, 能由不同的觀點來檢視稽核, 並加強了對大方向電子商務議題的重視。例如, 以往可能並不被強調的商品發展風險。更重要的是, 經由電子商務風險表的發展過程, 增進了管理階層管理電子商務風險的效果及效率。

5. 下一階段發展？

電子商務風險表及風險辭典都是有生命的文件，而它們的生命力藉著持續的發展與維護得以持續, 當有新的風險被發現或舊的風險已消失, 規劃定期去修訂風險清單。基於有些特定風險在電子商店不同的業務範圍內會有不同的威脅, 計劃繼續在個別的風險類別內, 對特定的風險下定義。與管理階層共同工作下, 將繼續尋找並辨認電子商務風險出現的表徵（因內部或外部環境的變動, 而引發新的風險或導致原有風險的改變）。

電子商務風險表將有助於預期並辨認風險發生重大變化，思考這些變化的發展，將對風險導向稽核功能的啟動，持續改善的要求，將不利的意外極小化，將可接受風險管理水準的策略極大化。

第四節　網路銀行的風險管理與內部稽核

一、網路銀行的風險管理

（一）網路銀行之興起

由於網際網路的普及，無論是個人或企業都可以非常容易地連接上網，隨著網路技術的不斷改進，網際網路也由原本單純提供訊息交流之功能，逐漸商業化。網際網路無遠弗屆的行銷功能及低建置成本，更吸引各行各業都希望透過網際網路進行商業活動，而造成全球電子商務時代的來臨。在進行電子商務交易的過程中，除了「物流」、「資訊流」外，也因金錢的收付而產生 「金流」，網路銀行即為 「金流」的一項重要流通管道。

就銀行而言，網際網路使得銀行與客戶之間的關係產生不小的改變，銀行服務有了新的管道-網路銀行，藉以超越時間與空間的藩籬，使金融服務無限延伸至各個角落。自從美國 SFNB（security first network bank）在網際網路上建立世界上第一個網路銀行之後，更帶來強大的競爭衝擊。目前各銀行無不積極研究如何透過網際網路提供各種服務，我國財政部亦要求金融機構在 90 年內需建置完成網路銀行且開戶數至少達 2000 戶，目前國內已有 39 家金融機構開辦網路銀行服務。

（二）網路銀行服務項目

通過網際網路，網路銀行可將金融服務帶入每一個企業、團體以及家庭中。透過全球資訊網的銀行首頁，一般客戶可以隨心所欲地查閱銀行簡介、新種業務、信用卡、營業據點的介紹，以及利率、匯率或金融行情。經過申請核准的網路銀行客戶，更可以利用連線服務安全快速地查看交易和餘額明細以及其他帳務性資料，甚至從事網路交易。低廉的網路花費結合多媒體的外觀，給予廣大客戶群超值、多元的服務，跨越傳統的時空束縛，提高企業形象和競爭力，並有效地提昇客戶服務品質。

根據調查目前網路銀行所提供業務功能，計有下列數種：

（1）查詢

存放款查詢、匯率利率查詢、黃金存摺掛牌查詢、基金淨值查詢、預約轉帳查詢、信用卡查詢、公債資料查詢、進出口業務查詢、客戶申請網路銀行服務項目查詢、投資理財試算等。

（2）申請

支票申請、金融卡掛失、電子憑證掛失等。

（3）檔案傳送

下載一般客戶帳戶明細、下載約定客戶、帳戶明細。

（4）網路服務

E-MAIL 註冊及變更、變更密碼、變更使用者代號等。

（5）轉帳

轉帳作業、預約轉帳、預約轉帳註銷、和台幣活期性存款轉無存單定存及無存單定存解約、外匯活期性存款轉無存單外匯定存及無存單外匯定存解約、變更每筆或每日累計轉出限額等。

（6）轉繳

公用事業費用、期貨保證金、信用卡費、罰單等轉繳。

（7）繳稅費

各類所得稅繳稅款、綜合所得稅結算申報採網路申報者自繳稅款等。

（8）信用卡安全電子交易 (SET)

（9）信託業務

員工持股信託業務。

（10）基金買賣

國內基金業務、海外基金業務。

（11）網路下單

證券交易業務、債券業務。

（12）網路銀行之成員

網路銀行在進行電子收付時牽涉許多成員，其中包括人與機器，謹說明其關聯性如下：

＊ 持卡人 (cardholder 即客戶)

在進行網際網路交易之前，必須先向認證中心（CA, 如國內之台灣網路認證公司）申請取得數位證書(certificate), 並且取得電子錢包 (e-wallet) 以安裝在個人電腦上。

＊ 廠商 (merchant，又稱特店，即交易認證伺服器)

廠商接收客戶之訂貨資訊 (order info)。在網路銀行系統設計中，此交易認證伺服器將可取得客戶之轉入銀行帳戶資訊。

＊ 支付閘道 (payment gateway)

支付閘道用以接收客戶之付款資訊 (payment info.)。在網路銀行系統設計中，支付閘道取得客戶之轉出銀行帳戶資訊，隨後並將此資訊傳送至交易認證伺服器。

＊ 認證中心 (certificate authorization，CA)

負責核發客戶、廠商及支付閘道的數位證書的公正機構。如台灣網路認證公司等機構，將在國內扮演認證中心的角色。在電子商務的標準架構中，銀行扮演的角色為廠商，為交易提供付款閘道，國

內的台灣網路認證公司則扮演負責憑證簽發單位。

網路銀行為配合客戶之需求與銀行管理及安全上的考慮，依不同作業性質，分別建置「連線交易伺服主機」(production transaction serve) 與中心主機連線，負責執行各類連線交易及安全控管，以及建置「全球資訊網伺服主機」 (world wild web server) 提供銀行首頁服務。再經由 ISP (internet service provider)連接網際網路，完成網路銀行整體架構。為網際網路安全控管，必需裝置防火牆 (fire wall) 以保護網際網路至內部網路間的安全，並保護內部交易主機的安全。

（三）網路銀行之安全控管

網路銀行基本上是建置於網際網路電子商務之安控模式架構下。在此安控模式的架構下，客戶資訊獲得隱密性的保障，資料不被纂改，可以驗證收發訊息對象的身份。更不必擔心對方會否認曾經接受或發送訊息。

而這些考量都是網際網路環境中必要的安控設計，也是支援、強化在虛擬空間中從事電子商務、金融交易的最佳解決方案。安控標準包括下列幾項重要安控需求：

（1）資訊隱密性：資訊不為不相關單位所揭露。

（2）資訊一致性：資訊在傳輸過程中不致被算改。

（3）辨識功能：對持卡人（客戶）帳號、及特店身份之辨識。

（4）系統互通性：符合電子商務標準之產品可相互搭配應用。

安控措施之細節詳如下述：

1. 主管機關對於電子銀行之安全控管規範

依財政部所頒定「金融機構辦理電子銀行業務安全控管作業基準」，對於銀行經由網際網路與客戶端電腦連線所提供之電子銀

行業務, 其安全控管作業須涵蓋交易面與管理面, 詳述如下表 5-1。

表 5-1 交易面之安全需求

防護措施	網際網路之電子轉帳服務
訊息隱密性	必要
訊息完整性	必要
訊息來源辨識	必要
訊息不可重覆性	必要
無法否認傳送訊息	必要
無法否認接收訊息	必要

資料來源：參考書籍 R2（十四）

2. 管理面之安全設計

網際網路轉帳交易之管理面安全設計詳述如表 5-2：

表 5-2 網際網路轉帳交易之管理面安全設計

防護措施	安 全 設 計
建立安全防護策略	1.建置防火牆、提供驗證與簽發電子簽名之安控軟體、以及線上監控軟體等。 2.使用User ID, 密碼, 電子憑證(存放於磁片)等存取控制設計。 3.簽入時間控制。 4.單次簽入。 5.控制密碼錯誤次數。 6.電腦系統密碼檔加密。 7.留存交易記錄與稽核追蹤記錄。 8.約定帳戶與限定金額等業務面控制。
提高系統可靠度措施	1.預備主機、伺服器之備援裝置。 2.建置病毒偵測軟體以定期掃毒。 3.更換應用軟體之預設密碼。
制定作業管理規範	1.制定安控機制。 2.撰寫客戶端之操作手冊及完整合約等。

資料來源：參考書籍 R2（十四）

(四) 網路銀行之風險

網路銀行之風險計有九種：

1. 作業風險

（1）安全風險

計有訊息隱密、完整、來源辨識、不可重複、無法否認等風險。因此要注意所使用的加密技術、認證功能是否完備。

（2）系統設計風險

即軟硬體設計上之風險。因此要注意網路銀行交易伺服主機、全球資訊網伺服主機等之安全防護、防火牆是否適用，交易軟體是否有適當之處理與控管。

＊ 操作風險

即於正式上線時對銀行及客戶端是否有足夠之控管，以維持交易正常執行與控管。

＊ 因客戶使用不當造成之風險

客戶設定密碼太過簡易以致容易遭人破解、未適當保管電子憑證、客戶未申請適當操作項目造成無法執行交易、錯失商機等。

＊ 由於銀行管理不當或疏忽造成之風險

未對試圖闖關者加以適當注意、未作簽入時間控制、未控制密碼錯誤次數及密碼加密、未留存交易記錄與稽核追蹤等。

＊ 系統維護風險

定時執行備份作業疏忽、未確實監控系統運作、未能確實控管系統異動所造成之風險。

（3）信譽風險

銀行提供網路銀行服務，因穩定性不足、處理速度緩慢或因系統安控措施不良造成客戶之困難或損失，將導致客戶不再使用網路銀行，甚至會造成銀行信譽受損。

（4）委外作業風險

網路銀行通常會涉及外部之服務如憑證機構、網路服務供應商等，對於該等作業常有斷線、憑證誤認等銀行難於控制之風險。

（5）法律風險

即銀行因提供網路銀行服務致客戶受有損害時，銀行應負之法律責任及義務。

（6）信用風險

即銀行因提供網路銀行服務，對每筆、每日交易金額如未作適當控制，或未落實覆核制度所造成之風險。

（7）流動性風險

由於網路銀行係提供二十四小時全球性不間斷服務，客戶可在任何時間、地點處理交易，因此銀行資金之管理相當重要，如未做適當之管理，將會造成銀行資金流動性不足，甚或因到期日控制不當而造成損失。

（8）利率風險

對利率敏感性資產由於資金流動而造成控管不當之損失。

（9）市場風險

未配合瞬息萬變的網路交易做適當的資產負債管理，所可能產生的風險。

（10）國家風險

由於網路銀行可以直接從事各國間金融交易，因此易遭逢國家風險，必須注意各國政經情勢並設定配額，以避免損失。

二、網路銀行之內部稽核

網路銀行業務對內部稽核是一大挑戰，稽核人員應就所查核之網路銀行衡酌其業務範圍、性質及風險作評估並訂定查核規範，對原已存在傳統銀行內之查核程序如可適用亦應一併納入。

網路銀行之內部稽核可參照中央銀行金融業務檢查處編撰「網路銀行業務查核項目參考資料」作為訂定各項查核規範之依據。一般而言網路銀行之查核分下列十大項：

（一）法規遵循

應注意網路銀行各項業務是否皆經主管機關核准，跨國業務是否符合當地法令，銀行內部規定是否配合修改，是否合乎公平交易法、消費者保護法及個人資料保護法等，因網路銀行而產生之電子貨幣是否依規定提存準備及對其資金運用加以控管，委外契約是否符合相關法令，疑似洗錢交易與重大事件通報是否建立陳報系統等。

（二）董事會之監督及決策功能

網路銀行各項營運措施是否經董事會審議及有無衡量穩健原則，對於經營網路銀行業務之風險是否適當規範並定期檢討改進。

（三）風險管理

是否明訂風險管理規範並建立風險管理制度，如訂定風險限額、交易限額及委外作業之風險控管等。

（四）內部控制

有關各項網路銀行業務之操作及管理是否完整、周延。

妥適之內部控制規範，對有關網路銀行業務之資訊系統及網路通訊系統之開發、維護、運作及其管理是否明訂符合內部控制原則之規範，以及是否涵蓋安全控管規章，委外作業是否訂定控管規範等。

（五）資訊、網路通訊系統及業務之安全控管設計

對於訊息隱密、完整、來源辨識、不可重複、無法否認等項目，是否設計周詳，軟硬體設備是否周延妥適，防火牆是否恰適，有關閘道是否適當控管，各種金鑰、基碼、密碼是否適當設計並妥善保管，使用者身份密碼設計是否妥當，客戶銷戶、停止使用之處理程序是否妥善等。

（六）提高系統可用性措施

是否有緊急應變計畫且定期演練，系統備援措施是否恰當等。

（七）客戶端作業規範

操作手冊是否完整，是否明確告知客戶權利義務等。

（八）與客戶、委外廠商或其他第三者之關係

是否訂定書面契約，是否清楚界定權利義務，受委託之廠商是否須提供內、外部稽核及金融監理機構所要求之必要資料並接受檢查。

（九）業務推展及行銷廣告

行銷廣告不可誇大，招攬客戶時要注意對其他客戶資料之保密要求。

（十）例外管理

是否建立監控線上交易之機制，對例外事件之追蹤與管理是否落實。

三、未來的展望

不久前，對於網路銀行的風險管理與內部稽核，在實務上究竟要如何實施才妥當，似乎還停留在紙上作業階段，即使認識到必須針對網路銀行業務預先做好規範，但總是理論大於實際。聽到國外的片段報導，感覺上似乎與我們相隔過於遙遠，且與日常生活並無關聯。雖然銀行公會已經訂立「金融機構辦理電子銀行業務安全控管作業基準」並經財政部核定請各銀行配合辦理，惟相關部門及銀行都還處於模擬、探索階段。

最近報端揭露一件歹徒侵入網路銀行盜取客戶存款的案件，該歹徒供稱其發現設有轉帳功能的網路銀行，只要輸入身分證字號及代碼、密碼即可轉帳，而一些存款人所設定的代碼與密碼完全相同。經過不斷嘗試後終於盜領成功。

此案例正突顯不論是銀行或是客戶都不能忽視對相關業務的安全控管。銀行應依據主管機關所訂規範及本身所開辦業務內容，衡量應建立之內部控制及管理和稽核機制，以降低銀行及客戶所可能面臨的風險。客戶也要正視可能面臨的風險，對網路銀行密碼、代碼、帳號等個人資料，須嚴守秘密不輕易外洩或遭人輕易猜中外，也應避免透過供一般公眾使用的電腦進行網路銀行交易而造成外洩，並養成注意核對帳戶交易明細的習慣，則可避免存款遭人盜取多時尚不自知的風險。

值得警惕的是，在網路銀行業務陸續展開的同時，如果相關各方不加快腳步參考國外經驗及我國實務，訂定確實有效的作業規範及內控安全準則，銀行和客戶的各種有形與無形的風險必將迅速擴大。

第六章　電子商務風險管理之電腦模擬設計與分析

第一節 電子商務風險分析

在評估個別風險的重大性與可能性，實在是非常有價值的工具，經評定為最高度的風險（分為高度、中度、低度三級）時，將它標示為「關鍵」風險。當將關鍵風險與經評定為對電子商店單位及功能具重要性的電子商務流程連結，可歸納出以下兩類具有稽核優先性的分類：

（1）有多種風險威脅的關鍵電子商務流程。

（2）對多種電子商務流程具有威脅的風險。

風險管理分析方法包含「風險評估對象」、「風險辨認」、「風險估計」及「風險控制策略」四個程序。「風險評估對象」是企業在面對資訊系統時，應先確定那些資源或事件會產生威脅或弱點。「風險辨認」蒐集各種可能威脅資訊安全的有關資料，通盤分析以確認危險所在。「風險估計」則在評估風險事件的發生機率，瞭解可能引發的損失，作為風險衡量準則。「風險控制策略」是定義可能影響的衝擊，作為資訊安全決策的參考，建立有效、適用的企業安全政策。

在此我們將使用電腦來協助我們針對電子商務的風險的分析，並且配合電子商務的制度研擬政策來因應所可能產生的風險，以期望能將電子商務的風險降到最低，使得電子商務未來能蓬勃發展。

一、交易風險

我們先從最基礎的交易風險來審查，從事電子商務應公開有關交易的資訊，並使消費者能明瞭整個交易的過程、條款、及交易費用，讓消費者有權決定是否要進行交易。網路銀行為配合客戶之需求與銀行管理及安全上的考慮，依不同作業性質，分別建置「連線交易伺服主機」(production transaction serve) 與中心主機連線，負責執行各類連線交易及安全控管，以及建置「全球資訊網伺服主機」 (world wild web server) 提供銀行首頁服務，再經

由 ISP (internet service provider)，連接網際網路，完成網路銀行整體架構。網路銀行基本上是建置於網際網路電子商務之安控模式架構下。在此安控模式的架構下，客戶資訊獲得隱密性的保障，且資料不被纂改，可以驗證收發訊息對象的身份，更不必擔心對方會否認曾經接受或發送訊息。而這些考量都是網際網路環境中必要的安控設計，也是支援、強化在虛擬空間中從事電子商務、金融交易的最佳解決方案。安控標準包括下列幾項重要安控需求：

（一）資訊隱密性：資訊不為不相關單位所揭露。

（二）資訊一致性：資訊在傳輸過程中不致被纂改。

（三）辨識功能：對持卡人（客戶）帳號、及特店身份之辨識。

（四）系統互通性：符合電子商務標準之產品可相互搭配應用。

二、物流風險

研究其物流的方式，會產生一定程度的風險，並且是否有多重管道可以進行物流的運送，且判定所產生的風險是由誰承擔。針對物流如何能讓實物移動，讓貨物能安全準時到達客戶手中，避免不必要的違約，或者貨物的損失，此方面須針對宅配中心做評估。如此對物流風險做評估，才可以適時的提升配送機能，強化整個供應鏈的管理機能，以支援產品及服務行銷的策略性需求，強調時間及空間的效率特性。

三、實體風險

當有天災，或者人禍造成產品、或者其他設備損壞，導致商業損失。

（一）一般設備

這些設備可能面臨的威脅來自火災、水災、地震、炸彈及一些化學藥品的污染等。這些威脅發生時會癱瘓資訊中心，繼而造成停工的損失成本，或重建及測試的成本。

（二）資訊設備

資訊設備可能面臨火災、地震及人員安全管制不力的威脅。最重要是，資訊設備不能被未經許可者使用。

（三）軟體

程式遭使用者或程式設計師意外修改或破壞、被不安全程式影響而當機，利用備份資料時不正當使用資料、裝設新軟體或修改後的軟體採用了不安全的新程式碼，這些都是使用軟體的所面臨的威脅。

四、人員的風險

考慮其他第三者的生命、財產的風險，或者其他因人員疏忽所引起的風險損失。

（一）個人

競爭敵手指使員工偷竊資料、不滿離職員工報復、或為私利複製資料、協力廠商員工利用電腦使用權限偷竊資料。員工是否盡職管理系統？是否讓網路繼續正常執行？是否降低資料被盜用的可能性？都是個人威脅的考量範圍。

（二）其他必須考量的風險

欺騙與偷竊商業間諜盜取資料行為及如何保護個人隱私權等。

第二節 資訊風險評估方式

一、資訊安全風險評估

要去分析組織系統安全風險最好的方法是每一定時間便執行一次資訊安全評估。安全評估可以幫助我們定義、了解且量化資產的風險。要了解這些風險的第一個步驟，是建置一個安全的基礎架構。

現在有很多種的風險評估方法，但是大多都是用特定的方

法。在特定的方法中，有些是風險的存在，相信管理風險的存在，且介紹解決這些風險的方法。這些處理過程經常是一些最近所發生的安全事故，或者是一些新的交易問題。雖然這些方法應用在一些組織上，並不是很有條理，且可能錯失相當重要的交易。

一個完整的風險評估方法的討論是超出我們的範圍的，但是我們將著重在一般六個分析風險評估的步驟。風險評估的處理過程是建制一個安全基礎架構的一個重要的步驟，這跟商業所需要的安全機制是相關的。風險評估顯示出潛在的重要商業處理過程的機密性、完整性、可獲得性的衝擊。每一個安全性的控制都必須花費，且必須由商業所提供，使這個控制能得以實現。

（一）最基本來說，風險評估回答了七個問題：

1. 甚麼會出問題 (威脅事件)？
2. 如果出問題了，那麼最壞的狀況是甚麼？
3. 多久會發生(週期)？
4. 如何確定答案能夠解決以上三個問題？
5. 哪些風險可以被移除、減輕或者被轉嫁出去？
6. 又會損失多少？
7. 影響又有多大？

（二）在真實的狀況下，風險評估是非常複雜的，但是我們可以利用一般的方式來評估風險，以下是風險評估所包含的六個步驟：

5. 清單、定義和要求。
6. 弱點和威脅評估。
7. 控制評價。
8. 分析、討論和說明。
9. 訊息。

10. 顯示。

風險評估的處理應該包含技術性的和非技術性而獨特的輸入，這將幫助我們確信這些可以包含整個風險。

二、風險評估的方式

（一）Tree Analysis：這個方法著重於過程或事件發生導致特殊的狀況。

（二）History Analysis：這個方式是週期性的檢查過去發生事件來決定再次發生的機率。

（三）Human-Error Analysis：這個方法是檢查人員干涉或者錯誤所可能產生的衝擊。

（四）Probabilistic Risk Assessment：這個方法是檢查機率，事件的結合將導引特定條件。

（五）Failure Mode and Effects Analysis：這個方法是檢查系統中的每一個潛在錯誤狀況，來決定其有多嚴重的影響。

（六）HAZOP(Hazard and Operability)：檢查過程和工程的意圖以評估潛在危險，能夠在設計規格中由偏差產生的方法。

三、風險評估的步驟

（一）第一步：清單、定義和要求

風險評估處理的第一個步驟將幫助我們了解每一項資產項目的公式，準確的評估風險潛在的衝擊是必要的。

1.首先在評估之前，必須先確認有風險的業務。以下是應回答的問題：

（1）我們如何增加收入?

（2）我們通信的主要方法是什麼？

（3）在哪裡存儲關鍵資料，並且如何修改那些資料?

（4）在哪裡存儲原始碼，並且如何修改它?

這個網站的資訊一定是適時和精確來使顧客滿意的，否則顧客將開始選擇其他的交易。關鍵的客戶資料被儲存在資料庫內且只有客戶可以修改資料。在總部開發者的網路次網上存儲備份的原始碼。只有在為了公司的品質保證才能修改或變換。而開發者本身不能去修改原始碼。

2.一旦確定了評論商業過程方法，查明那些資產組成的過程。除了實體的資產，例如服務器、發送程式、郵件服務器和網路的服務器以外，也應該考慮下面的範圍：

（1）網路服務和協定。

（2）遠程途徑位置。

（3）在內部網和網上傳播怎樣的資訊。

（4）誰應該能存取，並且在什麼時候他們應該能存取它。

當創造資源表時，需要確認它是徹底便於管理的。省略重要的資產將導致一個製造瑕疵的決定過程。但是公開下的一切將使整個過程笨拙和不很可能完成。

（二）第二步： 弱點和威脅評估

在第二步中，小心徹底的分析系統的弱點，且了解弱點被利用的可能性。確認所包含的風險不僅只有電子風險(網路攻擊)，也包含一些實體風險，如用磁片偷取資料或者系統被修改。

除了分析連結端和網路層次的威脅以外，在系統的應用程式方面，例如網路服務器和電子郵件的服務器，今天大多數成功的攻擊是透過 misconfigured 或 unpatched 的網路服務器。這包含了大多數的網路和系統攻擊點。

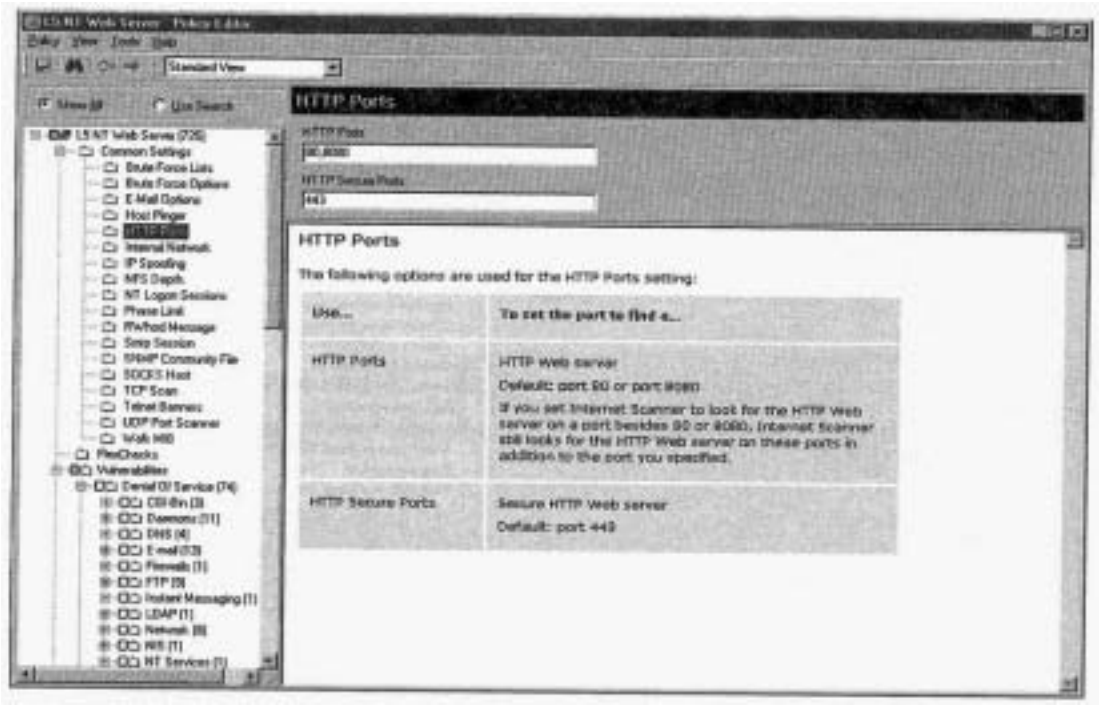
透過許多工具的協助可使這個評估過程自動化操作。雖然手動方式能為系統分析所有的弱點，但是使用自動化工具有助加速分析，在系統方面至少產生可知的弱點報告，可作為分析

起點。下一步將討論一些自動化操作的掃描工具。

1. Internet 安全系統

Internet 安全系統(ISS), 產生了包括網際網路掃描器和系統掃描器的掃描產品的 SAFESuite 。網際網路掃描器是網路掃描器，而系統掃描器是主要的掃描器。網際網路掃描器是掃描第一個可應用於網際網路的，且今天仍然是最流行的應用軟體之一。這個掃描器可用於 Linux 和 Windows 系統，並且能夠下載評價版本於 www.iss.net。

圖 6- 1 AFESuite 畫面



資料來源：參考書籍 R2（二十四）

網際網路掃描器，含有違約策略以及設計自己習慣策略的能力。 ISS掃描器看起來知道所有安全架構的弱點。提供需要固定弱點和威脅的所有資訊。目前網際網路掃描器可找到 728 個弱點，包括：

(1) 47個後門

(2) 50個daemons

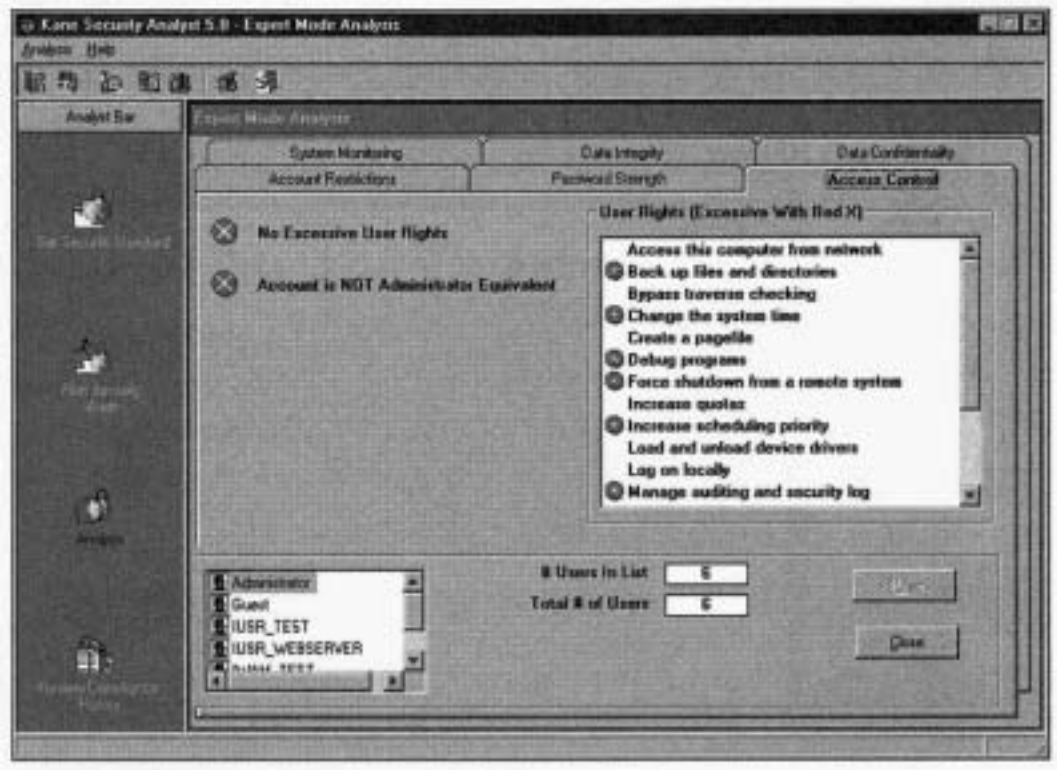
(3) 38個cgi-bin

(4) 51個NT-pacth

(5) 50個e-mail 檢查

2. KANE 安全分析

圖 6- 2 Kane 安全分析畫面



資料來源：參考書籍R2（二十四）

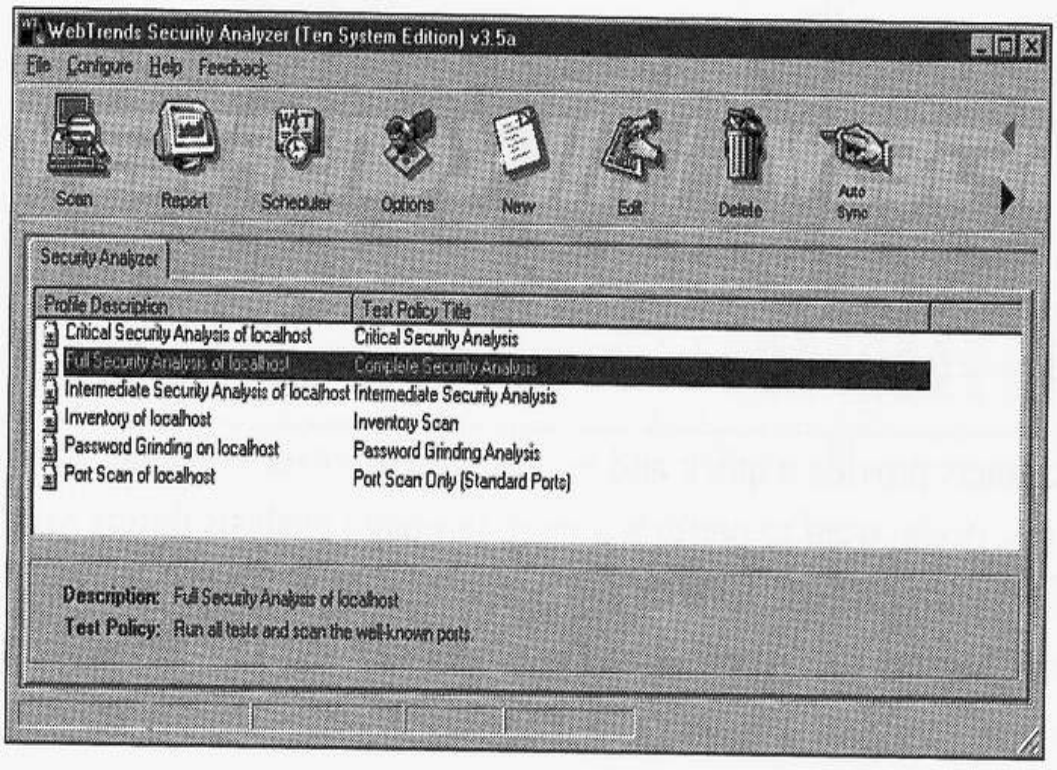
Kane 安全分析，可由Intrusion.com獲得。在六個評論安全範圍分析系統 ：密碼長度、存取控制、用戶帳限制、系統、資料完整性和資料的秘密監控。這個掃描器不尋找特殊設備的弱點，但是為系統的稽查提供一個基礎。

Kane 安全分析用安全標準來 preconfigured, 但是, 這些能夠對企業作為適當修改。

3. WEBTrend 安全分析

WEBTrend 安全分析, 可在www.webtrend.com獲得, 可以掃描linux和windows系統、防火牆、和路由器等大多數的威脅和弱點。也可以由webtrend看出configuration 的文件, 且可以知道一些在linux 和windows系統的弱點。

圖 6- 3 Webtrend 偵測畫面



資料來源：參考書籍R2（二十四）

Webtrend 可以提供我簡單的去閱讀有關弱點的描述, 也提供建議步驟來解決風險和幫助我們強健我們的系統。

Cerberus 網際網路掃瞄器可以在www.cerberus-infose.com獲得。

Cerberus 網際網路掃瞄器是一個功能強大且免費的工具。它可以掃瞄出126個web的弱點，包括以下幾個：

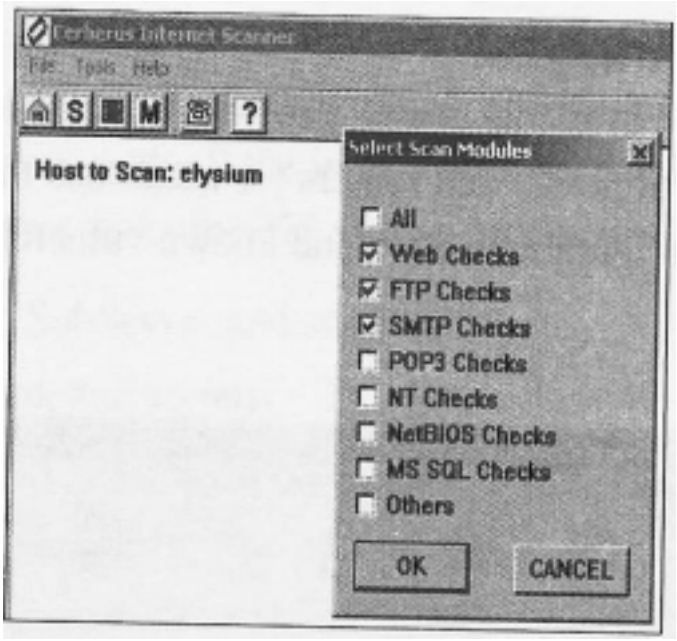
(1)21個smtp 弱點

(2)7個FTP弱點

(3)19個資料庫伺服器弱點

(4)超過60個NT伺服器弱點

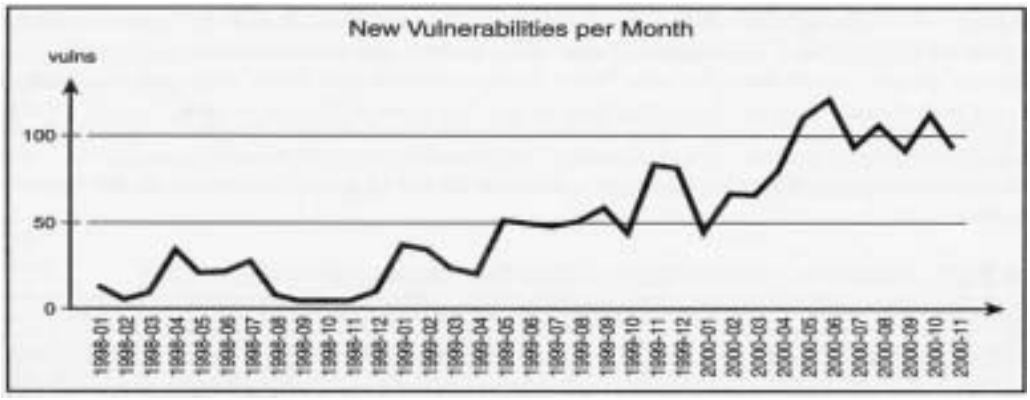
圖 6- 4 Cerbrus 偵測畫面



資料來源：參考書籍R2（二十四）

弱點掃瞄器可以提供快速且簡單的方式去檢查網路上或系統上的弱點。找出弱點之後，應該定義出那些威脅攻擊系統成功的機率。計算這些機率的方式有很多，我們可以建立 tree analysis 且去討論可能導致弱點被攻擊的機率。我們也可以分析過去攻擊系統或者曾在網際網路上討論的報導。如CERT、SANS和Bugtraq database等組織都有提供相關的資訊。我們可以在Bugtraq database 找到一個每月份弱點數愈來愈多的例子，如下圖6-5：

圖 6- 5 分析弱點數例



資料來源：參考書籍R2（二十四）

（三）第三步：評價控制

表 6- 1 可能的控制選擇和相關的花費表

Threat	*Possible Controls*	*Cost*
Unauthorized user modifying the database	Strong access controls	$25,000
Unauthorized user viewing the contents of the database	Data encryption	$5,000
Attacker or malicious user gaining control of the Web server	Firewall	$10,000
	Intrusion detection	$10,000
	Intrusion prevention	$10,000
	File integrity	$8,000
	Installing upgrades and patches	$10,000
	OS and server hardening	$20,000
Denial-of-service attack on the Web server or mail server	Perimeter protection (firewall or router)	$10,000
Email viruses	E-mail anti-virus	$5,000
	Client anti-virus	$10,000
	Strong policies on e-mail attachments	$100
Attacker or malicious user spoofing e-mail address from Anson, Inc. mail servers	Proper configuration of mail server	$10,000
	Monitoring outbound SMTP connections	$50,000
General network attacks	Firewall	$10,000
	Intrusion detection	$10,000
	Intrusion prevention	$10,000

資料來源：參考書籍R2（二十四）

在這個階段中不做出任何決定；這裡需要集體研討潛在的保護措施和控制相關費用。控制的方法可能是一種技術（如執行一個安全產品），或者基礎的策略（如需要雇員需求和證明網際網路途徑正確）。我們將把威脅的危險減少至零；剩餘危險幾乎總是將存在。風險評估過程允許我們控制所有的剩餘風險的數量。分析弱點和潛在的安全措施和控制將使我們了解業務和相關的風險。這會使安全投資充分發揮，獲得更多的利益。很多電子商務的焦點都是在當威脅產生時重點處理和修補漏洞。但這不是最有效、安全或者成本效果合算的方法的。表6-1可能的控制選擇和相關的花費表，為一虛擬公司所做的表格，顯示出可能的控制選擇和相關的花費。

（四）第四步：分析、討論和說明

潛在的控制需要看風險值的陳述，控制的費用只比獲得和執行的費用多，包括操作、保養、可用性、scalability、和展示的花費。

根據分析第三步所產生的清單，以風險評估過程（第二步）期間搜集的資訊為決議的基礎，決定執行那一項控制。在分析和決策上包含各式各樣的人們，從管理代表到商業過程所有者，其中技術和非技術層面兩者都有。參與分析和決策讓每個人得到所有權感。另外商業過程所有者最好理解這個過程並且控制它，使它在我們的環境中將獲得最好成效。這個步驟的最後階段是要透過用文件說明，使過程成為正式完成。文件越好，那麼下次就會越容易處理。表6-2選擇控制和相關花費表，為一虛擬公司可選擇的控制和相關的花費。

表 6- 2 選擇控制和相關花費表

Threat	*Selected Control(s)*	*Cost*
Unauthorized user modifying the database	Strong access controls	$25,000
Unauthorized user viewing the contents of the database	Data encryption	$5,000
Attacker or malicious user gaining control of the Web server	File integrity Installing upgrades and patches OS and server hardening	$8,000 $10,000 $20,000
Denial-of-service attack on the Web server or mail server	Perimeter protection (firewall or router)	$10,000
E-mail viruses	E-mail anti-virus Client anti-virus Strong policies on e-mail attachments	$5,000 $10,000 $100
Attacker or malicious user spoofing e-mail address from Anson, Inc. mail servers	Proper configuration of mail server	$10,000
General network attacks	Firewall Intrusion detection Intrusion prevention (host)	$10,000 $10,000 $5,000

資料來源：參考書籍R2（二十四）

（五）第五步：通訊

我們已經完成整個風險評估最難的部份，但是我們現在要去做最重要的步驟：把結果傳達給適當的團體。

傳送評估處理的結果用來確認組織所了解的風險，也能夠明瞭以前被忽視的弱點。這也有助於金融政策發展過程。這些結果必須被傳送到管理者、過程所有者、和使用者。最後的報告是我們獲得用戶的意識的方法，成功地幫助實現控制。

（六）第六步：顯示

隨時進行監控是很重要的，當我們組織改變時，威脅也跟著改變。我們的風險評估必須不斷的更新來保持相關性。當組織中主要的部份改變時，如變動電子商務所有人，我們必須重新去起動整個風險評估處理過程。我們的風險評估現在是完成了，我們可以了解對我們的組織和潛在的威脅且緩和，或者轉移有威脅的風險。

第三節 模擬結果分析

當我們分析完結果，可以了解整個電子商務所可能造成的風險，再根據風險的模式來制定因應的政策，當風險無法降低時，我們可以考慮加入保險或者其他可以轉嫁風險的方式。電子商務風險模擬將可以發揮下列之功能：

一、辨認對電子商店有重大妨礙的風險及確保上述風險於稽核規劃過程中已列入考慮。

二、促進風險管理人員在內部稽核或與管理階層討論中，對風險有更多之討論。

三、建立電子商店內部對風險變化之監控及立即辨認新風險產生之基本架構。

四、為管理階層及內部稽核對風險作預先的準備，而非等到風險已造

成效率降低後才有所反應。

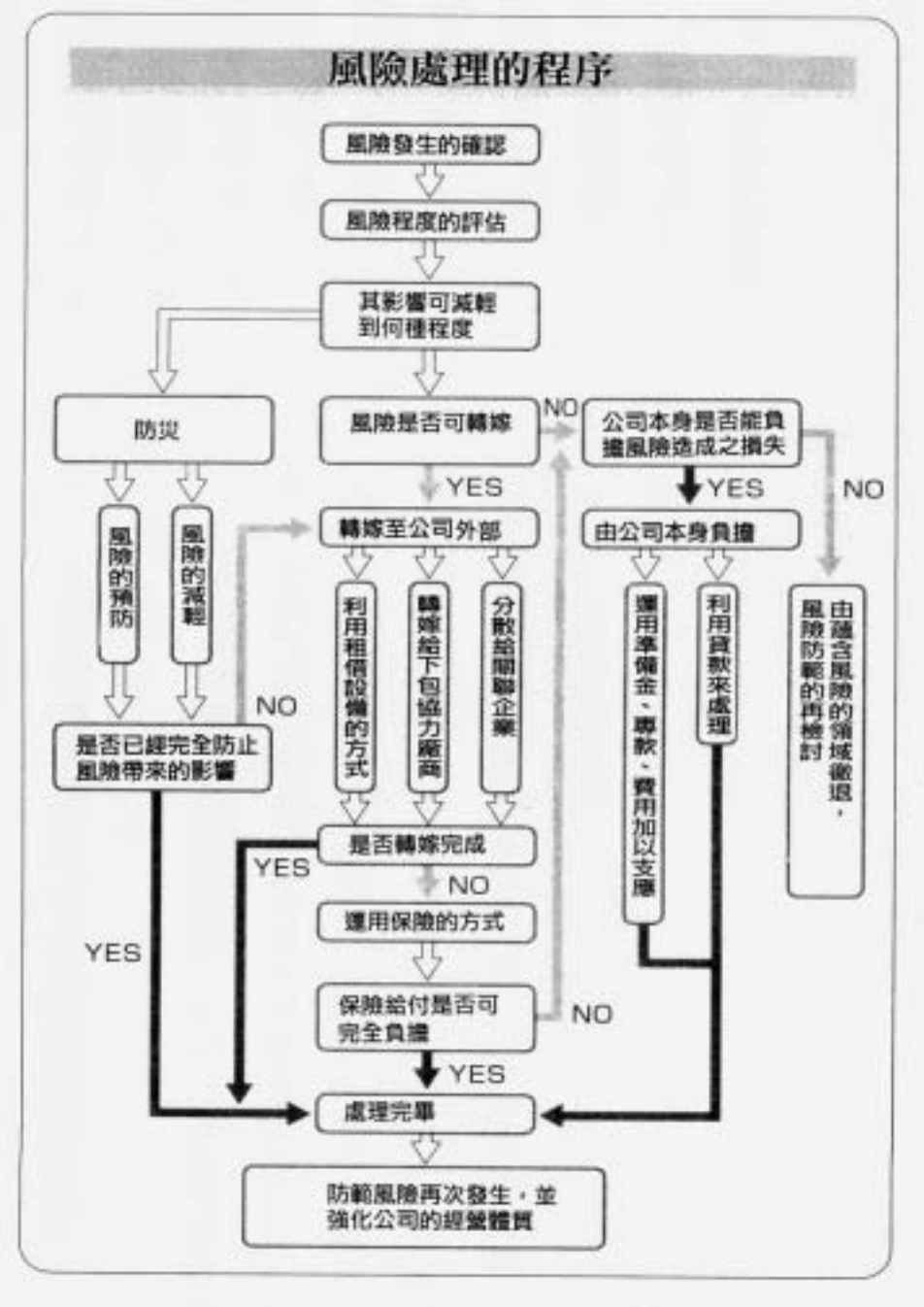
五、加強電子商務人員風險方面之專業知識，並了解那些風險對本電子商店具有威脅。

經由電子商務風險與管理之政策與制度模式之電腦模擬之後可以降低風險，並妥善處理各階層之關聯性，以及將營運目標與資訊技術之控制合為一體，使得電子商務更具推廣能力，可為企業帶來一股新的熱潮。圖 6-6 為整個風險的處理程序。

範例展示：

來源參考 IBM trivoli SecureWay Risk Manager 風險管理的全方位整合解決方案 http://www.tivoli.com/products/demos/sway_ov.html 點選其中的 Click to launch the way SecureWay overview demo 的圖示進入後，會檢查是否有安裝 java 虛擬程式，若以安裝則無此提示，若有則會自動安裝。之後會開始 loading demo images 讀取完之後會再問是否要讀取聲音，此時可有可無。進入畫面時在選擇 next 畫面中間會出七個圖示我們可以點選 PLAY AUTORUN LOOP 看全部的顯示，裡面會有詳細的介紹。

圖 6- 6 風險管理程序圖



資料來源：參考書籍 R1（四）

第七章 電子商務保險制度的可行性評估

因應電子商務及企業電子化的盛行，無論是企業或是個人均因使用新興科技而帶來新的交易風險，如駭客入侵或是病毒破壞等等。其所造成財產的損失或是責任的增加，是否可以透過保險機制的運用，來減輕或分散使用者及企業的責任？這都是未來值得關注的議題。在電子簽章法通過後，確立了電子簽章之法律效力，但目前 B2C 電子商務除了網路銀行及網路證券交易採 SET 及電子簽章外，多數交易在不可否認性上仍有疑義。在此情況下，保險制度在責任歸屬上仍有重大困難度，要推動電子商務保險機制前有必要先解決此問題。

每當資訊科技業者有新的商業經營模式產生時，一方面帶給產業無限的希望，另一方面也增加有別於以往的經營風險。如企業提供軟體租賃服務時，軟體租賃服務業者對於客戶資料毀損或是網路傳輸中斷等危險時，是否可以運用保險機制來分散風險？又因資訊通訊的發達，截取或重製他人資料變得輕而易舉，更大大增加了企業侵害他人專利或著作權的可能。檢視企業目前既有的保單，是否足以保障新興科技運用所帶來的危險？或是現有保險險種已不足以保障，而必須開發新險種以為因應？以下即簡單介紹電子商務經常發生的損失、責任類型，以及與傳統保單相互扞格之處。

本章針對電子商務保險制度的可行性進一步探討。分為四方面說明：第一節、電子商務稽核及風險管理：簡要說明電子商務稽核及風險評估後，為何需要電子商務保險導入的原因。第二節、電子商務保險功能：進一步說明電子商務保險功能及其制度建立。第三節、國外電子商務保險種類：介紹現行美英各國電子商務保險施行狀況及承保項目簡介。第四節、國內電子商務環境及未來保險可行方向：說明建立國內電子商務保險基礎建設的政府角色。最後，第五節以電子商務保險辦理應注意事項作為本章之結尾。

第一節 電子商務稽核及風險評估

就前幾章提出的電子商務風險稽核的結果，可將企業電子商務平台的風險程度分為高、中或低。針對不同的風險程度可以有不同的管理風險的方法，例如，衡量的結果，若是單方面軟體保護措施不夠完整，可以藉由更換軟體或添購新的軟體來降低風險；若聘雇人員對電子商務系統操作不熟悉，則可以利用教育訓練的方式來降低風險。有時候添購新產品或新的硬體（如防火牆），也是降低風險方法之一。執行電子商務交易的企業，若對電子商務系統原理技術不熟悉，也可以利用電子商務外包(outsourcing)的方式來達到降低風險的目的，聘請專業的網路服務提供廠商(ISP)或應用服務提供廠商(ASP)來協助電子商務事項，類似實體產物下的保全制度。

以上降低電子商務風險的方法，都是針對系統本身安全性的補強。然而電子商務交易模式並非花費大量的軟硬體及教育訓練成本就可以高枕無憂的，仍有其不可確定的風險存在，例如新種病毒傳播、冒牌使用者的介入、私人資料外洩、資料遭纂改及破壞、交易導致第三者責任問題，這些狀況都需要一套風險管理機制來降低電子交易執行的風險，電子商務保險正是此風險交易下最佳機制。顧名思義，電子商務保險是保護電子交易雙方，包括企業或消費者，因電子交易造成財產損失或是責任增加，能夠透過保險機制的運用，來減輕或分散消費者及企業的責任。

第二節 電子商務保險功能

本節將討論電子商務保險功能，包括電子商務保險制度及其功能特性，並列出現行國外的公司保險保單所承保範圍：

一、電子商務保險制度

電子商務保險保障電子交易雙方所導致財產損失或侵權第三者的求償損失，是屬於傳統財產保險的範疇。和過去的產物保險最大不同點，在於電子商務保險在執行電子商務交易時，能夠針

對可能引發的各項風險，訂定詳細闡述保險條款，以補救過去財產保險含糊不清條款的不足。

最明顯的幾個例子來探討傳統產物保險不適用在電子商務交易損失的求償認定。例如傳統產物保險的「實體損失」(physical loss or damage) 的認定，在美國聯邦法院有案例法(case law)可依循，認為「實際損失」不應僅限於電腦電路系統實際、物質上的毀損，而是應該包括存取、使用及功能性的損失在內。但有些州的法院解釋行動電話授權密碼及資訊科技專利並不屬於有形資產的一部分(1997 年美國法院判決)。另外，「員工不忠誠」(employee dishonesty)通常也不被包含在財產保險的範圍內。就傳統標準商業犯罪險(crime insurance)方面，時間因素所造成的損失，如企業商業中斷或額外費用產生，也並沒有加諸在傳統保險範圍。此外，隱私權侵權、智慧財產權違反、專業責任、媒體責任等傳統商業第三責任險都沒有針對電子商務交易特別考量而設計，一旦法院具體判定賠償要求時，保險功能是否能顯現出來是一大問題。這是為什麼要訂定專屬的電子商務保險的原因。

就電子商務保險制度而言，我們可以就政府、企業、個人等三個角度來探討。

（一）就政府角度：

政府應該建立可發展電子商務保險機制的推手，以迎合世界潮流。電子商務發展有助於國家經濟競爭力提昇，如何讓更多的企業或消費者去進行電子交易，除了基本的資訊基礎建設外，也必須使電子商務交易機制能獲得更多認同。過去五年來，在企業對企業(B2B)電子商務交易額快速增加的同時，相對的企業對消費者(B2C)的交易比率則無明顯增加，一部分原因是消費者對電子商務交易信心不足，交易風險認定過大所致。政府鼓勵電子商務保險制度的設立，將有助於電子商務交易風險降低，間接推動國家電子商務發展。再者，國外先進國家如英美等國的保險

業者，早有將電子商務保險項目納入承保範圍，幫助企業在風險承擔上多一種選擇。對於國內企業逐漸邁向全球化(globalization)且電子商務交易的無遠弗屆，政府應該從政策及立法雙方面來建立起電子商務保險的環境，讓電子商務保險制度能與世界同步，並保護本國企業不受過大的交易風險。

（二）就企業角度：

企業經營的型態正逐步在改變，由於企業環境的變遷，過去曾是企業經濟命脈的土地、人力、設備、資本等生產要素，現在都變得容易取得。相對這些有形要素而言，資訊資源反而是現在企業創造競爭優勢的基礎。為了避免過去重要的財產，如土地、人力、設備、資本等的損害，很多企業都會對其財產加以保險來減輕財產意外損失的壓力。同理，現在企業如何保護自身資訊資源安全，將資訊資源投保，更顯示其重要性。電子商務是創造企業競爭優勢的利基，同時它也帶來更甚以往的經營風險，例如軟體租賃服務時，對客戶資料的毀損及網路傳輸中斷的危險。另一方面，資訊網路的發達，抓取或重製他人資料變得輕而易舉，更大大增加了企業侵害第三者專利或智慧權的可能。就 2000 年 5 月「商業保險」(business insurance)中的報告顯示，美國有 70%的大企業或是政府部門在過去一年中，曾遭受到電腦犯罪及安全上的侵害。這些攻擊及侵害是來自於駭客及病毒的攻擊，並且導致直接財產上的損失，如網頁的損害；或是第三人責任的危險，如竊取信用卡的號碼。這些都需要一套完整且適合電子商務特殊要求的保險機制來降低交易風險。圖 7-1 左半部顯示過去傳統企業資源要素避險措施，右半部則顯示現今電子商務網站企業著重在資訊資源的保障，及包含第三責任險在內，適合的避險保險範圍。

圖 7- 1 傳統企業與電子商務網站企業資源要素避險措施

傳統企業	要素	電子商務網站
資訊險(侷限病毒險)	資訊	左列第一、及未列之第三責任險及罪險、勒贖險
股市、債市、期貨、選擇權等避險措施、金融險、再	資金	
財產保險、設備險、產品責任險	設備	
勞工險、意外險、壽險、犯罪險	人力	
火險、水險、房屋險、地震險	土地	

（三）就個人角度而言：

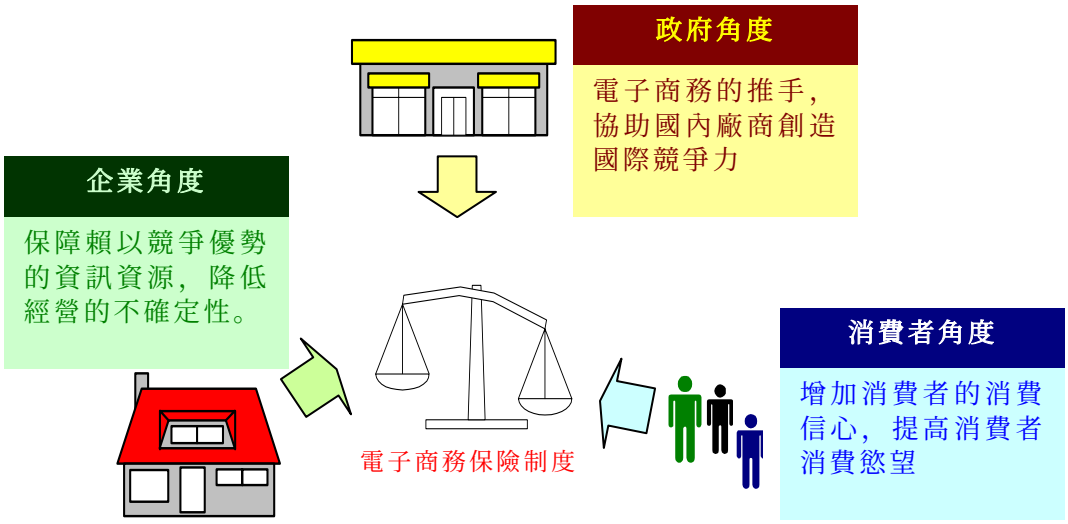
這些次數頻繁的網路不安全事件，使顧客對 B2C 的電子商務交易望之卻步。網路保險將可逆勢操作建立起顧客的信心，因為電子商務網站保險將交易雙方風險都納入承保範圍，大部分的風險由交易雙方移轉至保險公司，間接地鼓勵消費者在低風險下消費。

聰明的消費者將會選擇有安全制度的電子商務網站來消費，例如有建立安全標章的網站。這些安全標章一部分是安全的資訊加密傳輸的認證標章，如 HiTrust 的 VeriSign，它保證公司或團體所設立的正牌網站，且具有保密機制(SSL)保護消費傳輸的個人資料（如信用卡號，帳號，密碼等）。另一種安全標章是保證電子商務網站的安全性達一定的程度，如美國 BBBOnLine、TRUSTe、Web Trust 標章，國內 SecureOnLine、台北市消費電子商務協會 Secureshopping SOSA、經濟部標準檢驗局 ISO 認證等。同理，未來電子商務保險也應必須朝向網站標章或採認證方式來執行，以建立消費者消費信心。

圖 7-2 顯示電子商務保險制度對政府、企業、消費者

三者之間的重要性。就政府角度而言，電子商務保險制度是電子商務基礎建設的一部份，並可協助國內企業邁向國際化之路。就企業角度而言，電子商務保險制度可保障賴以競爭優勢的資訊資源，降低經營的不確定性。就消費者而言，電子商務保險制度可增加消費者對電子商務交易的信心，增加電子交易的慾望。

圖 7- 2 電子商務保險制度建立對政府、企業、消費者的重要性



二、電子商務保險功能與特性

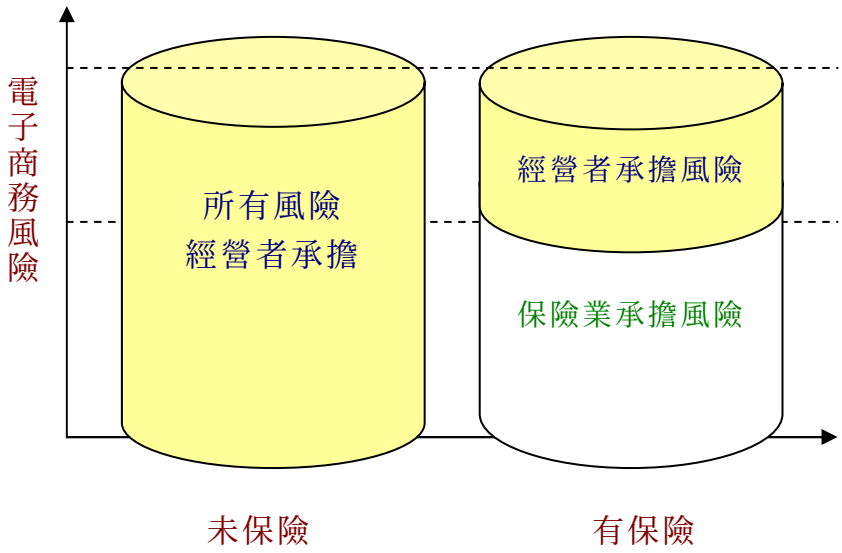
電子商務保險具備那些功能及特性，我們就購買者角度、販賣者角度、以及執行電子商務交易者角度來看：

（一）購買者角度：

電子商務保險的最大功能即是降低網站經營者的風險。這些風險無奇不有，包括病毒攻擊或第三者入侵所造成無法營業的損失、或是資料的損壞。其次，員工的不忠誠或是不可避免的犯罪行為介入也是風險來源。另外，網站經營者誤用別企業的專利或商標、智慧權的侵權行為，亦是不可

預知的風險。就圖 7-3 所示，左邊圓柱體是表示網站經營者無保險下，必須承擔所有不確定性的風險，這些不確定風險，少則令公司蒙受重大損失，多則足以讓整個公司倒閉。右邊的圓柱體表示經營者有承保保險，相同的高風險下，因保險公司移轉了絕大部分的風險，網站的經營者只要承擔小部分風險，對經營者而言，經營不須花太多注意力在風險控管，可專注在主業產品研發或銷售技術上。

圖 7- 3 電子商務經營者承保電子商務保險將可降低經營風險



（二）販賣者角度：

過去產險產品並不適合使用在電子商務站經營上，因為電子商務經營有其獨特的風險內容。因此，保險公司若只販賣傳統的產物保險，將無法吸引電子商務業者去購買。就經紀人而言，推銷這些商品將是事倍功半。另外，過去層出不窮的保險條文紛爭也造成保險業者與保險者之間的困擾，保險者近期也都更進一步檢視保單詳細條文，對於含糊不清的產物保險，保險者是退避三舍。對於電子商務保險而言，電子商務風險明訂於保險條文，將會吸引更多相關資訊產業經

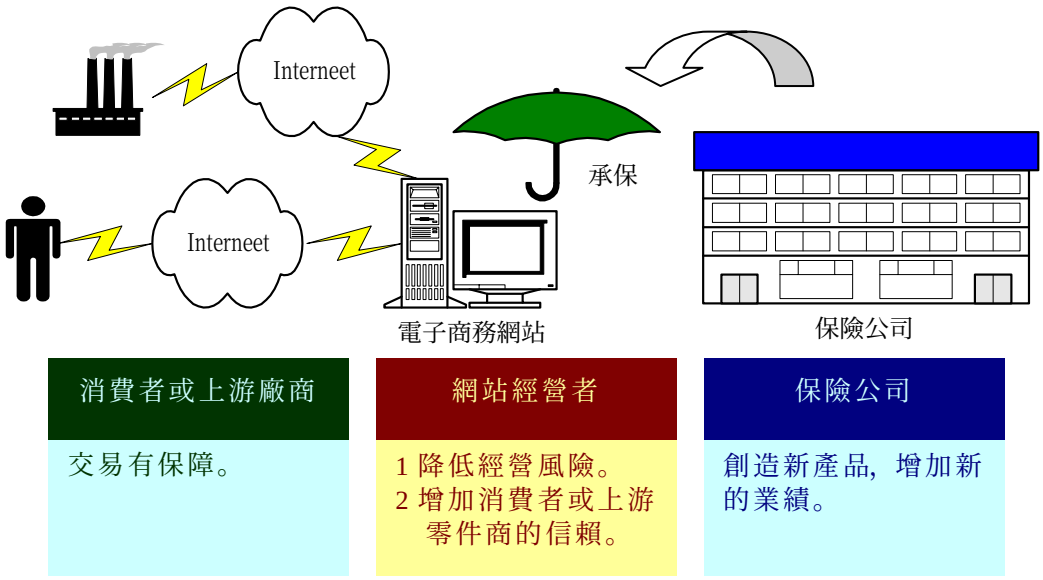
營者的進一步青睞。相對保險公司而言，公司創造出新產品，有助於公司業績發展；同時，因為明文規定風險範圍，也有助於責任的釐清。

（三）執行電子商務交易者角度：

電子商務保險除了第一人責任險外，一般還包括第三人責任險。所謂第三責任險是包含電子交易執行者蒙受損失的賠償問題。第三人可以是交易的顧客、上游供應商或其它社會大眾，當他們在執行交易時，所引起的糾紛時，電子商務保險可以確認責任賠償的問題。如此，可讓交易雙方都有風險上保障。

電子商務保險的功能，可從購買者、販賣者、及交易者來說明。其中購買者通常是指電子商務網站經營者而言，電子商務保險具備(1)降低經營風險、(2)增加消費者或上游零件商的信賴等功能。販賣者是指保險公司而言，從此角度來看，電子商務保險是一項新產品，增加新的業績。就交易者如消費者或上游廠商或經營者本身而言，電子商務保險使得交易更有保障。

圖 7- 4 電子商務保險辦理將創造三贏的局面



三、電子商務保險之類型

電子商務保險是屬於財產保險的範疇。傳統上關於財產保險所提供的保障，大致可區分為財產損失及責任保險二部分。所謂財產損失保險是指有形資產上的損失或損害；而責任保險則是要保人對於第三人，依法應負賠償責任且受賠償請求時，其所應負的責任轉由保險人來代為承擔。所以，在電子商務保險亦可區分為財產及責任保險二大類。電子商務中之財產損失危險，仍是指有形資產的損失或損害；而電腦責任危險常見的有下述三類，均是因網路活動，都可能造成企業對第三人責任的發生原因。

(一)系統危險(system damage/security threats)

因為電子商務的執行與運作發生系統中斷的風險。如因為安全系統被破壞所造成的傳輸中斷, 或是因為第三人(如服務提供者或是維護系統)的錯誤所發生的中斷, 均屬於這裡所稱的系統的危險。公司可能會造成第三人硬體或是軟體的損失，或是因為服務提供者或是支援系統者的過失或是不小心的錯誤，而造成自己系統的損失。或許這些損失也會因為自己員工的疏失或是因為第三者的攻擊，如駭客或是病毒等。以 2000 年 5 月「商業保險」(Business Insurance)中的報告顯示, 美國有 70%的大公司或是政府部門在過去一年中，曾遭受到電腦犯罪及安全上的侵害。這些攻擊及侵害是來自於駭客及病毒的攻擊，並且導致直接財產上的損失，如網頁的損害；或是第三人責任的危險(third-party-type risks)，如竊取信用卡的號碼。

(二)智慧財產權的請求(intellectual property claims)

有關商標侵害或是商標淡化的情況。諸如：未經授權使用網域名稱、標語的使用而侵害商標權、使用超連結技術而跳過他人網站的首頁、利用視框連結技術而造成商標或是其他的侵害等等，均是新興產生的責任型態。

(三)媒體責任(media liability)

這裡是指對於企業的毀謗及侵害隱私等危險。目前系統服務提供者或是因為使用 cookies 技術, 追蹤使用者的交易記錄或是其他的資料等等，均會造成使用者或是消費者隱私權的侵害。

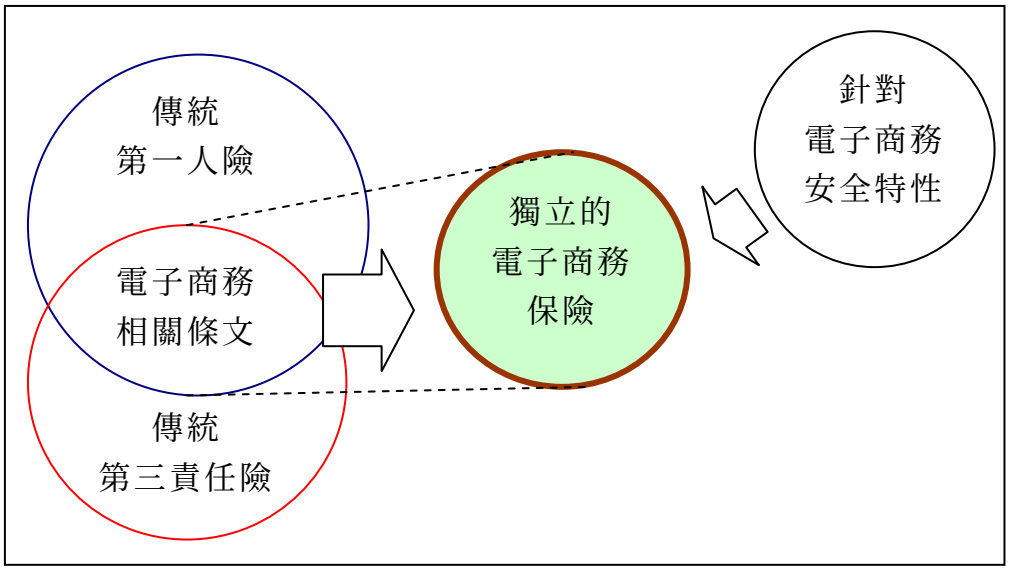
第三節 國外電子商務保險種類

本節針對現行國外電子商務保險種類進一步探討。另外，說明電子商務保險承保範圍及項目。

一、現行國外電子商務保險種類

現行國外電子商務保險種類可分產物保險內含電子商務險與單獨電子商務保險兩種。前者是將過去產物保險增加適合電子商務經營風險的明文到保險範圍內。而後者則是節錄過去產物保險及傳統第三責任險外，還包括其他相關電子商務安全獨特條款，如圖 7-5 所示。

圖 7- 5 獨立的電子商務保險

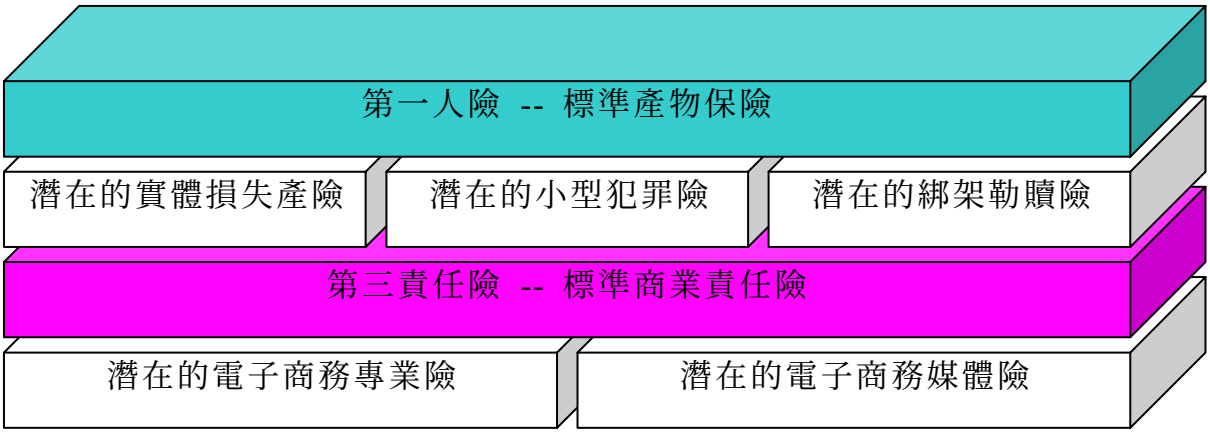


過去產物保險及第三責任險並非針對電子商務交易而設計，因此很多條文都只是含糊帶過，不一定適合電子商務網站經營者的保險的需要。經營者若同時承保過去完整產物保險及第三責任險並不適合，只需針對電子商務相關的風險承保即可。國外另一種獨立的電子商務保險是針對電子商務交易而設計，融合過去第一及第三責任保險的結合，並加上電子商務特殊字眼及特別條款，使承保者明確認知保險範圍。

目前英美兩國企業大都比較偏好保產物保險內含電子商務特別風險條文。原因是這些企業過去都有承保產物保險，而後因為導入電子商務網站經營，而導致公司交易風險的增加。為彌補過去財產的不足，會要求保險公司在已承保的產險另訂相關電子商務的條文。

針對保險經紀人而言，由於他們對舊有產險比較熟悉，因此大部分的經紀人也比較傾向推銷舊有產險加上電子商務條文。然而，若對一個純粹電子商務網站經營者而言，傳統產物保險加上各式各樣第三人責任險都承保，將造成很多不必要的成本浪費。美國有很多學者都比較傾向成立單獨的電子商務保險，這樣的保險只針對電子商務經營風險而設定，並且改進產險及傳統第三人責任險不足的部分另外提出條文說明清楚。

圖 7- 6 獨立的電子商務保險範圍



一個獨立的電子商務保險範圍應包含第一人險及第三責任險兩大項，如圖 7-6。其中第一人險是指承保自身財產安全，有標準的產物保險、潛在實體損失險、潛在的小型犯罪險、以及潛在的綁架勒贖險等。而第三責任險則是保護第三者不受網站交易而蒙受損失或受傷，有標準商業責任險、潛在的電子商務專業險、以及潛在的電子商務媒體險。

二、電子商務保險承保範圍及項目

目前對於企業所使用的保單，多屬於標準化制式的保單。所以企業如果因為網路活動而發生直接財產上的損失或是承擔第三人的責任時，則應先檢視目前的保單是否有涵括這部分的保障。

發生直接財產上損失的情況時，或許會有保單條款字義認定的困擾。美國法院即遭遇到對於資料、資訊或是其他網站上電子功能的毀損，是否屬於傳統財產上的損失爭執不休。美國聯邦法院在 2000 年 4 月 Arizona 的判決中認為：「實際損失(physical damage)不應僅限於電腦電路系統實際、物質上的毀損，而是應該包括存取、使用及功能性的損失在內。」然而其他的法院判決則認為，行動電話授權密碼及資訊科技專利並不屬於有形資產(1997 年美國法院判決)。美國有許多的保險人也有提供關於電子資料處理(electronic data processing；EDP)保險(endorsements)，其明白聲明提供有關電腦系統的保障。但是針對這一部分，目前並沒有一個統一的用語來承保，所以，未來在發生糾紛時，對於怎樣的資訊或是系統應該在承保範圍之內，即發生爭議。另外，雖然有形資產沒有實際損害的發生，但卻發生有形資產使用上的損失時，則應如何處理。簡而言之，就是對於使用上不便或是不能提供使用所造成的損失，是否理賠，亦有認定上的困擾。

經上所述，可以看出企業因網路活動而造成的財產上損失，對於「損失範圍」的認定，目前仍屬模糊不清的階段，表 7-1 為英、美、澳三國保險業者對電子商務保險一些實例。

表 7- 1 英美澳三國保險業者對電子商務保險實例

保險業者	保險名稱	第三責任犯罪險	員工不忠誠	企業中斷&額外費用	敲詐險	專業險	媒體險
美國部份							
AIG	NetAdvantage Pro + Internet Professional Liability Policy	無	無	無	無	有	有
AIG	NetAdvantage Security + Internet and Computer Network Security Policy	有	有	有	有	無	有
AIG	Net Advantage Liability Internet and Professional Security Liability Insurance	部分	部分	無	有	有	有
AIG	ProTech Technology Liability Insurance Policy	無	無	無	無	有	有
Chubb	Cyber Security	有	有	有	有	無	無
Chubb Executive Risk	Safety'Net Internet Liability Insurance	無	無	無	無	無	有
Hiscox	Hacker Insurance	有	有	有	有	有	有
Legion Indemnity Company	INSUREtrust Electronic Information E&O (EIE&O) Liability Policy	部分	部分	無	無	有	有
Lloyd's	Computer Information and Data Security Insurance	有	有	有	有	有	有
Lloyd's (WISP)	Website Crime & Intranet Insurance	有	有	有	有	無	無
Lloyd's (Besso)	Technology, Media and Professional Liability Insurance	無	無	無	無	有	有
Lloyd's (JLT Risk Solutions)	E-Comprehensive	有	有	有	有	有	有
Marsh	NetSecure	有	有	有	有	有	有

(續上表)

Media/Professional Liability (Gulf)	CyberLiability Plus Insurance Policy	無	無	無	無	有	有
Royal Surplus Lines	Computer, Telecommunications and Internet Services Liability Coverage	無	無	無	無	有	有
St. Paul	Technology Premier Computer Network Security Protection (Networker)	有	有	有	有	無	無
St. Paul	Cybertech+ Liability	無	無	無	無	有	有
Tamarack (Great American)	Dot.Com Errors and Omissions Liability Insurance Policy	無	無	無	無	有	有
Zurich North American Financial Enterprises	E-Risk Protection Policy	有	有	有	有	無	有
歐洲部份							
ACE Europe	DataGuard	有	有	可加	有	無	無
Hiscox	Hacker Insurance	有	有	有	有	有	有
Lloyd's (JLT Risk Solutions)	E-Comprehensive	有	有	有	有	有	有
Marsh	NetSecure	有	有	有	有	有	有
Park Insurance Services	Internet Insurance	無	無	無	無	有	有
澳洲部份							
Marsh	NetSecure	有	有	有	有	有	有
St. Paul	Technology Premier Computer Network Security Protection (Networker)	有	有	有	有	無	無
St. Paul	Cybertech+ Liability	無	無	無	無	有	有

資料來源：http://www.irmi.com/expert/articles/rossi004Chart.asp

第四節 國內電子商務環境及未來保險可行方向

本節將討論電子商務環境的基礎建設、誰最有資格辦理此項保險業務？茲說明如下：

一、電子商務保險環境與基礎建設

電子商務保險環境必須靠政府及企業等多方的配合，才能把電子商務保險的機制建立起來，其中政府更扮演關鍵的角色。政府應該致力於電子商務保險的基礎建設，如相關政策與法令的建立，此外，政府也是一個最佳紛爭解決的仲裁者。

國內於八月中旬，第一張電子商務保險單獲准開辦，這是電子商務保險的機制的一大突破。如此將可以吸引其它保險業者跟進。當然保險業者也可參酌政府所許可的保單項目及國外電子商務保險內容，然後創新並增加自己公司新的產品。

此外，政府應該積極鼓勵保險業者或資訊安全業者開辦此業務，例如從降低稅率或公益宣傳，讓全民都能了解電子商務保險的優點，進一步增加消費者對電子商務網站的交易信心。

由於網際網路無遠弗屆，跨國性電子商務紛爭或風險問題應值得注意。在審核保單時是否只考慮自身國情，或違反其他國家法律等，這在審查階段必須有專業的法律團隊一起檢視。另外，國外電子商務紛爭處理機制 (online ADR) 的引進，亦可進一步建立交易仲裁機制，來達到責任歸屬的目的。

二、鼓勵保險及資訊安全業者辦理電子商務保險

誰最有資格辦理此項保險業務？檢視我國目前的保單，尚未針對網際網路或是因應新興科技而設計，所以未來在這部分，應該是保險公司可以發展的空間。然而缺少精算資料、請求的頻次與數據，所以保險公司在定價部分是比較困難。另外，保險公司也會考慮到是否可以再保分擔風險，以目前全球電子商務保險尚在起步階段來看，全球的承保能量都是非常有限的。然而，經營電子商務及新興科技運用，產生許多不確定的風險，也不同於以

往保單所承保的標的，企業多利用合約來減少或降低自己的風險，如果能再加上商業保險機制的運作，相信會更有助於電子商務的推動。

保險業者在缺乏精算保費基礎之下，可以成立資訊安全部門，來衡量各種資訊安全上的風險，此外，也可以參酌國外的保單政策，來設計自己的產品。另外，資訊安全業者也是適合經營電子商務保險的公司，因為他們是最清楚資訊系統漏洞的地方。

第五節 電子商務保險辦理注意事項

一、保單內容項目定義

本節首先針對保單常見內容的名詞進一步說明：

定義 1—「虛擬企業」

架設在網際網路上的電子商務公司需要風險管理的策略，保障資訊資源在所有其他在網際網路上的虛擬企業公司中傳遞時的安全。聯繫網路與非網路的虛擬企業是靠組成完整的資料和系統可獲得的東西的電腦和設備所組成的。這包括所有遠端和本地的使用者，網路操作中心，網站，遠端區域網路，資料保管區...等等。虛擬企業也包括外包公司的關係像資訊服務提供者(ISPs)，私人網路供應者，主機／排列的設備，遠端備用支援，遠端監控和保養的供應者...等等。網路設備由外包公司的顧問和顧客和販賣者/供應者的管理也是虛擬企業管理的一部分。由於內部的信任的連結和永久／虛擬的網路節點，ISP 的長途電信服務提供者和網際網路主幹的供應者也許已經有所有虛擬企業當中最大的方向。

定義 2—「公司股東」

牽涉電子商務的公司必須有責任去不惜一切代價地保護它公司的股東。任何的電子商務經營模型，公司股東的名聲都可能在任何情形中遭到損害，對可能的傷害包括財政損失，名

譽損失，和信用損失。股東團體包括顧客，供應商／供給者、股東／投資者。其他的股東團體可能包括董事會和一般公眾。

定義 3 —「第一者損失」

如果牽涉到電子商務的公司對它的資訊資源遭受到直接的財政損失，這就是第一者損失。舉一個例子，假如 X 公司有一個網站或者公司網路遭到病毒或者駭客／破壞者的攻擊，X 公司會因為復原和恢復自己的資訊資源所需的費用而遭受直接的財政損失。因為這些被保險的設備和資料的損失都是有限的，所以第一者損失比第三者責任的索賠容易管理和估量出來。

定義 4—「第三者責任」

如果牽涉到電子商務的公司造成或者允許傷害到另一個公司，被傷害的公司將可以有第三者的索賠。由被其他公司傷害的索賠包括資訊損失、財政損失、名譽損失，或者顧客和其他的商業關係的損失。被傷害的公司能夠保留法律責任，予與正式索賠或者訴訟。

舉個例子，如果駭客／破解者攻擊 X 公司的網路，而且發動網路攻擊到其他擁有者的網路(這叫作「島跳攻擊」)，靠使用 X 公司的網路對其他網路擁有者發動攻擊，駭客／破解者看起來好像是 X 公司所批准的使用戶。任何來自攻擊者產生的損害將追蹤回 X 公司並且他們能就其他人遭受的損失保留法律追訴權。從這點向前看，X 公司在所有聯繫這個網路世界的攻擊中，將會被視為危及的關鍵點而且他照樣能保留法律的追訴權。

因為這個潛在無限範圍的傷害，第三者責任索賠在電子商務的世界中是最複雜且最危險的損失類型。第三者損失的情形在網路世界中是不誇張的。X 公司是否該負釋放惡意病毒的責任，如果 X 公司的網路設置安裝是不穩定的，危及到顧客的系統的問題？及 X 公司是否是 ISP 或者網路服務提供者，它是否

能保證連線到電子商務網站和公司的區域網路的信任？

定義 5—「駭客」

駭客即是對電腦和系統進行破壞的人。駭客沒有惡意意圖，而且避免所有破壞活動可能對其他人產生重要的損害。通常好奇心、知識和教育激發是驅使駭客去探索他們欲破壞的主要系統。

定義 6—「破解者」

破解者是有惡意意圖的駭客。破解者破壞電腦和系統以獲得未經許可的控制權或者產生其他擁有系統者的嚴重損害。權力、貪心和報仇激發破解者利用被他們犧牲的系統創造輝煌的成就感。

定義 7—「電子商務危險管理」

在單一風險管理解決方法之下，標準化的各種管理方法聯合商業和科技設備，包括活動設計來保護和控制電子商務和公司電腦的操作中所有關鍵性的區域。包括組織和契約的控制、資訊和網路安全控制、人力控制、策略和程序的控制，還有人身安全控制。這是唯一方法去結合傳統保險、風險管理、商業諮詢和資訊安全最好的元素。

資訊安全 + 傳統風險管理 = 電子商務風險管理

識別 + 分析 = 估價

保護 + 避免 = 損失控制發展

控制 = 順從

回應 + 轉移= 回應和轉移

定義 8—「危及點」

當一個未經許可的人靠著破壞安全和存取控制來進入網路或者電子商務的環境，未經許可的存取特定模式將成為危及

的關鍵點。危及點可能產生在包括社會工程、資料的存取或者技術／電腦妥協的任何類型攻擊。當考慮充分的保護，發現和回應策略的時候，這是一個很重要的電子商務風險管理的概念。在電子商務發生損失之後，決定危及的特定點將是決定第一者和第三者損失的程度的關鍵，而這些都是電腦調查人和法庭等專家們的工作。如果 X 公司決定危及點引導對內部關鍵性的資源明顯的損害，將需要對特定的設備做保存和恢復的努力。如果 X 公司發現一連串的第三者損失的危及點，X 公司可能會保留對這些損壞部分的法律責任。

定義 9—「惡意的程式」

未經許可的入侵意圖，包括在一個系統裡的軟體或者韌體（framewave）。例如，特洛伊馬病毒或者其他病毒。

定義 10—「生命週期的風險管理過程」

所有的電子商務都需要生命週期的方法實行風險管理。這個方法考慮到電子商務處於固定生命週期發展的狀態，再造工程和修正。由於公司的電子商務從概念到初始發展，生產和維持演變而來，企業廣義的風險管理辦法在每一個層級都需要應用。完整的生命週期過程會提出批評電子商務的元素，包括進化，使商業目標進化，事業形態改變，迅速改變技術，外包關係中的變化，物質的位置改變和擴張膨脹，且改變國際看法。

二、投保注意事項

本章節將針對電子商務保障細項內容說明：

（一）員工忠誠險

為了防止在交易進行當中現金被竊盜及銀行的盜賊之風險，財政機構是第一個購買犯罪保險的機構。之後，透過雇員的偷竊或當實際發生竊盜時不實的描述，造成失竊率很輕易的上升。保險項目的定訂，是依防止雇員的不實及偽照之風險。在 20 世紀中，保險項目的四大考慮要素，(1)運送過程中、(2)

生產廠址、(3)雇員的無忠貞、(4)雇員的偽造，這四項要素被整合在所謂的銀行整體契約裏，也是大家所知的忠誠契約。一個忠誠契約的首要目的要包括金錢、安全感和雇員從老闆那裡偷的其他的資產，所造成的直接損失。

然而，在現今整個網路架構環境裏，這種網路機構可以避免一些損失，不用造成一些資產的實質被偷負擔。在網路安全上，光只是查閱或者拷貝資料的侵害，就足以造成很嚴重損失。這些契約成為了大部份財務機構在保險時所要保護的部份，都和過去傳統的資產和債務的保險項目有很大差別。在許多權限中，財務機構所附帶的忠誠契約，是管理的必要條件。

傳統的忠誠契約及犯罪策略，有一些重要項目有侷限性，不是按照新興電子商務出現的風險來考慮的。例如，忠誠契約和犯罪策略都將有關任何機密或業主情報的損失，排除在保險項目之外。這樣在本身遭竊盜損失時的保險項目上，產生了很明顯的差距。此外，傳統忠誠契約和犯罪策略，將任何可能直接或間接的損失的因素，都排除在保險項目之外。雇員不誠實或者敲詐類型的情況，造成商業中斷的現象，都不列入保險的範圍之內。數位簽章的到來，更顯示出個人的信用在慢慢的喪失中。在過去，若要借款，必須顧客和借主在財政機關面對面的進行交易。借主要知道要貸款者的財產，然後依財產多少來立契約擔保，契約的訂立必需要有誠實可靠的公證人署名，契約裡要求的每一條借款的保險，都必需符合忠誠契約裏條文的規定，像偽造或假冒相似的情況，也必須符合滿足商業的犯罪政策，以減少被保者所造成的危險事件的增加，然而隨著數位簽章的到來，整個處理過程就可以在場所外來進行，在實際上，借出方沒有相關的律文可以依賴，且在律文上沒有規定要貼上一個固定簽章。

在傳統的忠誠契約上，並無其它分歧的狀況。假如有個制度准許存取業主到顧客及第三個者的資料，則任何由此制度所造成的損失，將被排除在保險範圍之外。因此，必需持續透過

網路交易的顧客或買主，風險將超過他們既有的交易及所造成的損失，在傳統的忠誠契約之下，沒有任何的保險項目可提供。另外，此契約不包含由使用信用卡所造成的損失，另外其它的主要差別，不使用卡片的交易方式，比線上交易付費方式較易被接受。

在忠誠契約的例子裏，財政機構在信任風險上有附加危險。在不履行低信用保險業的貸款，或因起源於不誠實的履行貸款，而信用評比低之間，實際上是沒有什麼差別的。在後來的例子中，或者借款的主管因收賄於借款人的一些佣金、不適當的酬勞，而共謀勾結，或者由借款人某種騙局策略及偽造，以致借款的主管變成了受騙的犧牲者。這個商業或信任的風險不同於偶發的風險，因為風險可能隨著欺騙、未經授權或未預期的事件而提升，隨著主要領域的投入保險而降低。承保人和再保人所關心的重點是潛在風險的聚成及累積，會曝露出單一電腦同時攻擊多數的受險人的可能性上升。當產品在研發的過程中，可理解的恐懼可能會有負面衝擊的影響，尤其當承保人和再保人面臨像網際網路那樣普遍現象時，網際網路將全面性曝露保險業者的資訊，也增加一些困難使用傳統方式測量的新危險。透過例子，“I Love you”病毒據估算將近造成十億元的損，比許多自然災禍更加的嚴重。新病毒的指數成長，由於網路和機器的全球連通性的連接，其所造成的災難，等值於地震、風暴或者水災。

（二）電腦犯罪險

在七十年代後期，犯罪保險市場首先提供了電腦犯罪保險的相關領域。在這之前，員工使用電腦系統來偷竊的犯罪行為，可能被註明在員工不信任契約條款的抬頭下面，但是，大部份的電腦犯罪的形式，都涵蓋在傳統的保險契約保護之下。新的保險領域範圍，主要是依據北美及其它國際間的銀行，對於風險管理的需求來發展。在新興的電子銀行業者長期存在有文件偽造的情況下，因此致力於"電子偽造"範圍的政策定訂。

這樣，保險的範圍仍然限制了"直接的財政損失"的大部分，導致明定”資產”的損失，典型地有價值或者可透過談判解決的僅有項目，包括現金、安全等等。保險範圍也包括了軟體、資料、電子通信(包括電話)和軟體的惡意的破壞之欺騙性操縱的危險。

三十年以前，技術非常的不同。電腦系統是專用的，並且涉及保險商和公共機構的主要危險是" 局外人"能突破他們的電腦台系統。甚至那時，思索了把病毒引進機構的系統。必須把病毒實際上引入這個機構的專有本地地區，或者從它的辦公室引入廣域地區網路。存取公共硬體設備的控制是首要的安全策略。系統是專用的，且員工幾乎可專門的使用。今天，資訊技術的資源是全天候都可以上網的。Intranets、extranets 和 Internet 都貫穿所有的公共建設及事業。因此，有上網路使用瀏覽器的每個人，在無形中都擁有專用系統的通路到一個公司的網站系統。

在傳統電腦犯罪策略中，把員工和授權的用戶排除在保險的範圍之外。此外， 像商業犯罪或者忠誠的契約一樣，傳統電腦犯罪策略也特別將機密資料的遺失排除在外。

大多數傳統電腦犯罪策略，都有對電腦病毒入侵電腦造成的損失做投保。然而，並沒有考慮到新的狀況，整體的網路環境裏，處處都存在有電腦病毒及時時都有駭客不良的企圖的電腦攻擊的可能。

過去，在大多數傳統電腦犯罪策略下，外部的駭客或破壞者要進行破壞，必須存取一個系統，和把病毒引入目標公司的專有系統。此外，假如駭客入侵系統，或者病毒的竄入造成系統當機，這些必然的任何形式的損失都沒有涵蓋在保險範圍之內，是它產生的利潤或者產生的額外花費的商業中斷損失。在今日世界中， 許多新增的商業是在網路線上經營，這是傳統電腦犯罪策略中的另一個明顯縫隙。

不論是否是線上經紀人或其顧客想要存取他們的帳，和一天 24 小時、一週七天都要進行商業交易，或者提供網路銀行服務的銀行，當他們的網路操作關閉若干個小時，就可能在他們的收入和名譽上造成摧毀性的衝擊。最初，電腦犯罪策略僅僅針對於主要銀行而產生。之後，在財政機構和商業的組織上都更寬廣受到歡迎。電腦犯罪策略幾乎都提供當忠誠契約用，且由相同的承保人所立下。

不論它是否涉及電腦系統的使用，雇員不誠實的風險，仍然通常將被包括在忠誠契約的雇員不誠實部分之下。不受電腦世界的發展而受影響是保險範圍中一個重要的要素，因為會動用的保險的範圍，就是犯罪者使用一些欺騙性的手段。網際網路是雇員用它來向老闆進行犯罪的一項簡單的工具。應該注意的是在許多情況中對" 雇員"的定義, 已經有一些眾多延伸的改變，如職訓中的雇員，甚至現下可能包括合約職員、顧問及保管人等等。據估算有高達 70%以上的美元價值，用來索賠雇員的不忠貞的條款。這個百分比現在已隨著電腦犯罪增加而降低。 然而，雇員詭計似乎是是許多年來保持損失的主要來源。因此，一個有電腦的風險之保險產品，必須徹底認識到總體的風險, 才有意義。電腦犯罪的保險範圍, 當有欺騙的準備措施、電腦程式的修改、或者資料的假操縱時，或許可以保護投保人付款或者傳送資金的風險。同樣地，不管是否真正由投保人收到或者由寄送，增加的保護可用於由欺偽性電子通信產生的損失。

一個電腦犯罪策略的其他條款可能包括程式的惡意變更或者破壞、電子媒介和資料的破壞、透過電腦病毒及資料檢驗和重建的費用。然而，策略將典型地排除由這些，或者其他任何間接或必然事件產生所造的損失。

保險範圍也將一些為了達到廉價銷售而開發的不實軟體程式排除在外，因為像這樣欺騙手段的風險，若有一大群相同的保險業者的投保人，就有很大的影響。

（三）職場或專業責任險

在很多情況下,「新」經濟中所興起的責任險，是將在「舊」經濟中已經存在的那些做進一步的擴展。如果顧客由於資訊不充分而導致處理錯誤、或者信託者責任的違反而造成被信託者的損失，這跟是否是「舊」或者「新」的經濟體制並沒有很大的關係。然而，動態的電腦世界將造成這種很大風險。

例如，一間提供理財服務的公司可以透過網際網路行銷到全世界，雖然製造了一個世界性、且空前機會給更多有必要此資訊的顧客，但是這項進步同時也造成另一方面的責任問題，這些理財公司必須橫跨多重的管道來處理各國不同的法律上、管理上、隱私權上及其它公司承諾上的爭議。

當一個理財公司所提供的資訊有任何小錯誤，這可能造成使用此網站的所有全世界顧客蒙受損失，像這類損失是因為理財公司專業上的疏忽或專業知識不夠所造成，顧客若追究這損失的責任時，這便是職場的另一個潛在的責任。

職場責任險是針對公司「專家」系統無法提供正確專家的專業訊息所造成的損失賠償，能分擔部分「專家」疏忽的風險管理。

（四）企業負責人責任險

電子商務和網際網路的發展已經對企業的管理造成很大的衝擊。我們可以從幾個方面來探討：

首先，企業必須付出更多資訊科技的成本。例如企業的資訊基礎建設、資訊安全的措施、資訊設備的採購與不斷的更新、資訊內容的維護與廣告等，這些都是顯而易見的成本。假使這些成本沒辦法增加公司的利潤或是降低公司的成本，這將造成股東們的反彈行動。

其次，公司必須用更嚴格的尺度來建立本身經營制度。尤其必須面對下列主題，如隱私權、資料安全、內線消息、商標

權的保護、以及智慧財產權的保護等問題。

企業的負責人面對網路世界的不確定性，更加重其經營的負擔。如何能快速反應及運用資訊技術進步所帶來的競爭優勢，且避開企業經營不利的要素將是企業主管最頭痛的。我們可以從市場上本來很多 .com 的公司迅速消失情況來推論，一位網際網路或電子商務的主管策略將對企業的生存或股價的保衛，具有決定性影響。

（五）結語

隨著資訊科技的進步，不管是社會或是企業機構越來越依賴資訊技術了。這是因為資訊技術所帶來的利益遠超過她所帶來的風險。但這並不表示她的風險是可以忽略的。相反地，我們所倚賴的資訊技術所帶來的風險更甚以往，有很多領域若沒有這些資訊系統將無法繼續生存。這些領域將隨著時間而成長，並且更依靠資訊技術而存在，即使可能會隨著資訊複雜的本質而資訊濫用或甚至導致失敗。

在某些情況下，企業的弱點被利用代價是非常高的，有時候並非單一公司所能吸收與承受。因此，在這逐步發展的電子商務世界裡，對於保險業者及投保者兩種身份而言，他們更應該去了解電腦系統所存在的風險，並確認那些電子商務風險項目被置於保單內容？那些項目沒有被包含在內！同時一個保險業者也應創新保險產品，避免公司本身的市佔率受到別的公司的侵蝕。

另外，被保險人和保險業者都有共同目標來保護網站的安全，並 一同管理經營的風險，彼此也一起分享經營的利益。這是因為沒有任何一張保單是所有的風險只由保險業者單方面來負擔的，例如機會的喪失或名譽的損害等。這些與被保險人和保險業者兩者都有影響，唯有互信才能互利，互助才能避免彼此危機。

總之， 保險將領導企業以更高的安全標準來稽核自身的

系統，並且對系統更嚴峻的控制。網路保險也對未來網路發展扮演不可忽視的角色，不但創造更安全的網際網路環境，而且亦可引起消費大眾對電子商務交易更深切的信賴。且國內 micro payment 的機制若能建立，對於每樣商品都能給予小額的保險，應可有效減低網路付款的風險，將有助於電子商務的推動。

第八章 健全我國電子商務風險管理制度具體建議

由本研究計劃研擬之電子商務安全認證，風險管理及交易保險架構圖看來，應足以建構安全的電子商務環境，如再邀請電子商務相關領域專家，就國家整體觀點，檢討現行政府的立法管理尺度、業者自律公約、公信力第三者的認證機制、資訊安全標準、電腦安全稽核作業、安全產品檢驗及認證、電子認證機構之建立、消費者教育及保護措施、執法機關科技偵防能力之提昇、仲裁制度、及國際合作等政策與制度面的課題，整合可行之電子商務管理之政策與制度模式。

根據專家顧問訂定之風險與管理的政策與制度模式，參考國際間已有專業機構開發之電子商務風險評估與管理的模式，設計電子商務風險與管理系統模型，並施行電腦模擬與分析作業，所得之電子商務風險與管理評量表資料，可供電子商務保險制度可行性評估研討與報告之應用。

綜合本研究計劃各項工作項目的完成，最終可以整理健全我國電子商務風險管理制度之具體建議報告。其短、中、長期目標，如表 8-1 示，詳細說明如下。

表 8- 1 健全我國電子商務風險管理制度之具體建議表

時程	具體建議政策與措施	主辦機關/協辦單位	參考備註
短程：	(1)培訓各公私機關資訊部門資訊安全長。	經濟部主辦，研考會協辦。	
	(2)成立電子商務風險管理服務中心。	經濟部主辦，財政部協辦。	
中程：	(1)成立電子商務評鑑機構(公正第三者)。	經濟部主辦，公平交易會協辦。	
	(2)成立電子商務店驗證組織。	經濟部主辦，消基會協辦。	

	(3)推動電子商務保險機制。	經濟部、財政部主辦，消基會協辦。	
長程：	(1)建議電子商務風險管理中心及保險機制納入國家資訊基礎建設範疇。	經濟部、財政部主辦，交通部協辦。	
	(2)促成電子商務風險管理中心以國家組織的方式積極參與 CIS (the center for Internet service)為國際性非營私公司組織(cooperative organization)標章服務工作(charter service)。(運作規範參考網站：http://www.cisecurity.org/)	經濟部主辦，外交部、消基會協辦。	

第一節 電子商務從業人員組織架構

◎具體建議：短程第一項

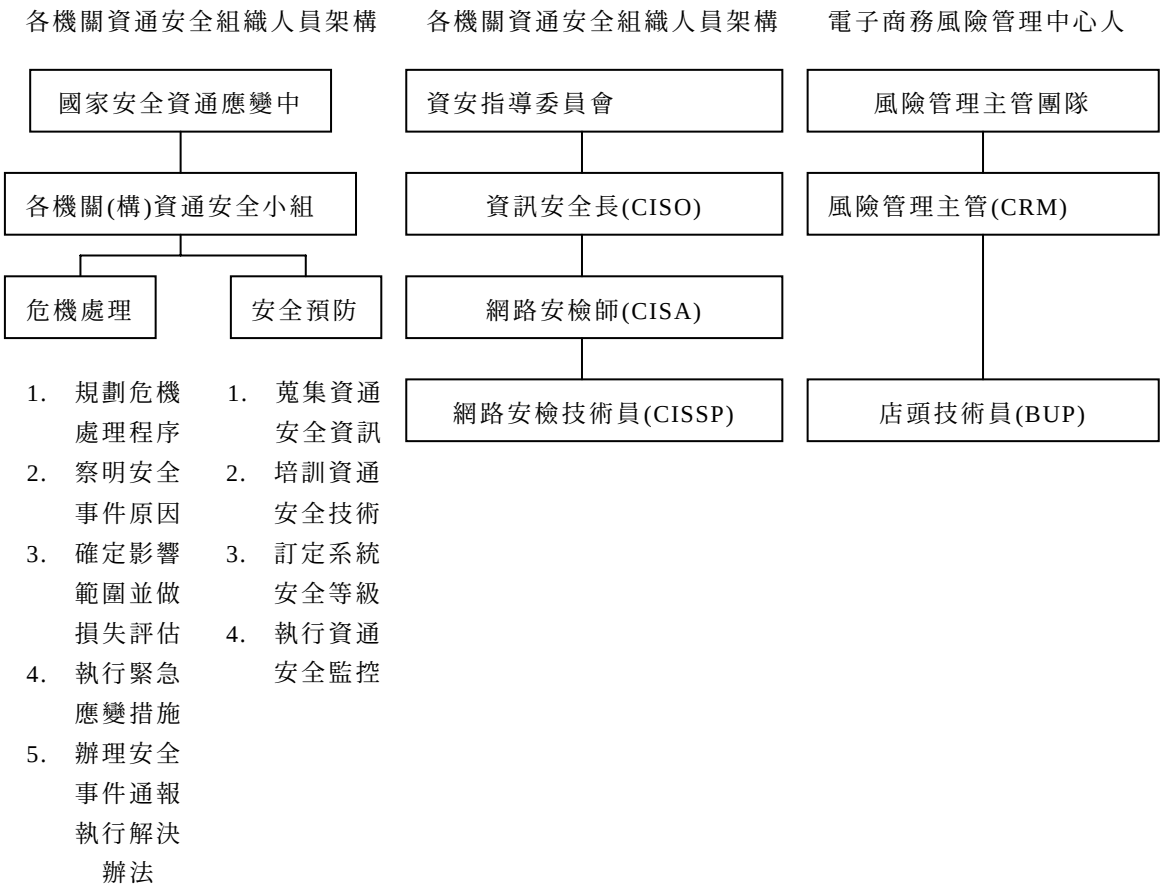
培訓各公私機關資訊部門資訊安全長計劃：

- 經濟部主辦，研考會協辦。

根據國家安全資通應變中心運作體系及執掌，如圖 8-1 所示，有關單位應施行各公私機關資訊安全長的培訓工作，因為資訊安全長的任命代表一個機構決定在業務操作之下，使資訊安全成為一個正式的作業程序，並進一步使之成為資訊安全的第一個指標。任命合適的資訊安全長這個步驟極為重要，不論是 50 人或者是一個 5,000 人的機

構，都要符合資訊安全長的規定，因為如果沒有資訊安全長的正式任命，其中的任務可能是由部門間抽調人員兼任，因此僅能做到支援工作而已。

圖 8- 1 電子商務安全組織及風險管理服務中心人員架構



所以，資訊安全長的培訓應為短程的第一項計畫。有關資訊安全長的行政功能職責及必要的諮詢工具要項如下：

一、資訊安全長(官)的行政功能

資訊安全長具有行政功能，以提供行政功能方面資訊。

（一）對資訊使用者提供必要的協助

資訊安全長幫助使用者理解資訊安全的重要，以及使用資訊安全的文化。資訊安全是嶄新的問題，所以資訊安全長必須鼓勵使用者增進他們的資訊安全警覺和風險意識，自我安排學習維護資訊安全的工具。資訊安全長要求全體職員遵守資訊安全作業，且確保他們熟悉資訊資源受威脅的來源和採取步驟，避免發生風險。瞭解資訊安全對於各級的新職員訓練的重要性。

（二）對高層管理報告有關資訊安全問題

資訊安全長應該作好準備提交半年或者一季一次定期的報告給機構的最高管理階層和並公告之。報告內容應指出如何控制資訊安全，以及主要資通安全最新的發展，並提出的任何風險變化的警告。同時為資訊安全作好應變的準備。

（三）編製資訊安全預算

應編製每年的資訊安全預算，項目如下述：

1.直接資訊安全職員的人事的費用。

2.其他相關工作的花費。

3.資訊安全硬體系統的增設費用。

4.資訊安全系統保固的費用。

5.專家顧問的需要費用。

6.新增資訊安全軟體產品的費用。

7.資訊安全訓練的費用。

資訊安全長應該幫助機構制定預算，作為每年預算編製過程的一個部分。

（四）機關內資訊使用者自我評估和考核

機關內資訊和系統的使用者需要定期完成兩項自我評估與考核要點。所有職員每半年應細讀這些自我評估與考核要

點。一是對於非技術的使用者，另一是對於技術的和半技術的使用者。技術或者半技術的使用戶比較可能完成自我評估。評估的目的是要獲得職員對資訊安全問題的知識回饋。

資訊安全長應該跨越整個機構鼓勵資訊使用者進行知識回饋和自我評估。培養職員確保機構和它的顧客資訊的安全當作是自己的責任，這將培養一個資訊安全文化。作適當監控和對其知識回饋和評論作出回應。

應該考慮堅持發給職員自我評估要點，作為其個人常用重要文件，作為職員的表現考核方法的參考。

（五）協調各部門在資訊安全問題有共同認識

資訊安全長必須確保資訊技術和系統相關的單位能夠緊密合作，增強資訊安全的認知。資訊安全長的責任可以與系統管理人和網路管理人重複。對於負責資訊安全的系統管理人和網路管理人和資訊安全長，密切的分工合作是十分重要的。

（六）負責資訊安全內外稽查單位連絡工作

資訊安全的策略和方針必須定期的稽查，可以幫助組織安全分級，保護組織的安全。資訊安全稽查必須配合計畫，並由那些了解資訊安全潛在危險且有經驗的技術人員來實施稽查。資訊安全長要負責與執行資訊安全的稽查工作。

（七）監控資訊安全策略的目標

執行資訊安全計畫是一個持續進行過程。運用安全意識支援訓練過程，需要一系列規則和方針的建立，以及對機構雇員活動的監控和標準原則的供應。監控不應該集中於捉住犯罪者，要能共同遵守資訊安全的程序，認識到資訊安全是機構的命脈。使安全與風險二者皆可支援機構業務的推行，平衡安全影響與風險的控制是十分重要的。

（八）定期舉行資訊安全會議

資訊安全長應該與所有組織內各單位和分支機構，定期舉行安全會議，討論資訊安全的問題。 並作正式記錄：

1.會議的緣由與目的

2.選舉會議主席

3.出席會議名單

4.議程

5.結論

6.誰負責進展達到的決定

7.下一次會議的日期

二、資訊安全長的職務和責任

資訊安全長的細部義務與責任，需要由上層管理部門清楚的建立和批准。

（一）資訊安全的首要責任

資訊安全長首要責任為管理機構內全部資訊安全，負責機構內資訊安全過程並發揮其有效功能。資訊安全長焦點應放在對所有資訊安全過程，和資訊使用者提出有關機構的資訊安全發展程序，並提供最好的保護。

（二）資訊安全問題上的建議和管理

資訊安全長的關鍵任務是要公告資通安全事件，並對控制人員和管理者提供建言和補救原則，對機構內涉及重要資訊安全事件的可能衝擊，斟酌資訊安全長所負的權限，描述機構的危險輪廓。

（三）資訊安全風險評估

資訊安全長負責對整個機構採取正式資訊安全風險評估作業，資訊安全風險評估是建立有效資訊安全計畫的第一步。沒有風險的評估，機構將不瞭解應該保護的是甚麼，應該執行

何種層級的保護和費用，並應按照機構財政資源以及作業的約束，適當把風險減少至可接受的層級。

（四）資訊安全程序的開發

有效資訊安全作業需要有正確的程序。必須經過各種業務設計過程的評估和批准，這些設計的資訊安全作業程序必須能在分離式的資訊系統中作業。其細節的程式開發將具備有ISO17799 和 BS7799 等高層級的資訊安全水準。

（五）在資訊安全問題上和其他組織合作

與資訊安全兼顧的組織互相合作和分享經驗。學習他們如何處理資訊安全的威脅，這可能是一個最有效的方法。資訊安全秘密在合作的資訊組織中是一個極為重要的步驟。資訊安全長將可在專業的網路上尋求協助，處理資訊安全事件。

（六）管理資訊安全策略

以今天的快速改變技術，資訊系統把新的挑戰送給資訊安全。它意味著資訊安全策略必須有規律地更新，資訊安全實踐才能夠跟上新威脅和危險。資訊安全長負責保存策略潮流和應該考慮可能對資訊安全危險衝擊的任何變化。如當機構改變它的商業實踐和潛在地增加它的資訊安全危險的層級，因此保持日新月異更新是很重要。為如此附加或者修改策略來獲得更新的公告或者控制的物體批准是一定要的。

（七）資訊安全計畫

資訊安全過程的重要部分是資訊安全計畫的發展。資訊安全長通常負責發展整個計畫。機構的商業計畫需要由一個補充和支援的資訊安全計畫來支援。這個計畫應該包括涉及資訊安全問題於機構的商業發展裡， 應該確定涉及關鍵的威脅和風險。機構的商業計畫應該包括資訊安全方面的部分，包含未來時期提出的資訊安全計畫並且應該詳述資訊安全威脅和危險，這要在商業計畫的時期補救。資訊安全計畫過程的大綱如

下:

1.發展具有細節的時間里程碑的計畫。

2.測量每一個任務或者目標的確定方法。

3.確定目前等級。

4.從目前等級到計畫目標改變的發展過程。

4.對工具計畫建立項目。

（八）處理資訊安全事變

資訊安全長的責任中特別重要的部分是當收到一個可疑或者實際的資訊安全事變的通報時應該立即回應。創造一個事變應變計畫，通常為了能夠把架構的回應應用於調查和糾正的過程。鑒於能夠透過資訊安全事變產生潛在的財政損失，通常使得適當的緊急評估由潛在風險的組成。在資訊安全事變中包含了下面的資訊安全事變處理的建議架構。

（九）檢視資訊安全問題

資訊安全長所注重的焦點，應該在於檢視機構內現存或者潛在的資訊安全問題。當檢視資訊安全問題時，資訊安全長應該使用與下面相似的過程大綱。

1.確定問題或者潛在的問題。

2.對問題帶來衝擊做分析。

3.確定選擇辦法和費用。

4.推薦和相關的辦法。

5.誰應該解決問題。

6.評估缺少矯正之後的衝擊。

（十）資訊安全長合格資格和經驗

資訊安全長的推薦資格和經驗如下：

1.資訊技術或者商業學習中的程度。

2.一個商業環境的經驗。

3.提供商業地區支援服務的經驗。

4.完整性的高層次。

5.造成信任和信心的能力。

6.對資訊系統，威脅和聯繫的危險友好資訊。

7.計畫和執行變化的能力。

8.解釋和用文件說明新概念和項目的能力。

9.加工商業系統和自動化的過程的知識。

10.在政策上的想像能力。

11.好的組織能力。

12.好的決議技巧。

13.品質控制過程的理解。

14.強壯的通信技術。

15.透過結果，表現管理的經驗。

（十一）任務聲明和資訊安全長的內部目標

作為資訊安全計畫過程的一部分，資訊安全長應該為直接支援機構的商業任務聲明和目標的資訊安全制定任務聲明和內部的目標。這些要適合於任一個機構的需要。 資訊安全為任務聲明和內部目標的建議如下：

1.任務聲明

資訊安全長:為機構的資訊安全管理中的可測量提供有效和改進的計畫。

2.內部目標

（1）碰到資訊安全威脅和危險。

（2）確認衝擊。

（3）支援商業目標。

（4）增加對顧客服務評價。

（5）出差導致的安全衝擊減到最少處理。

（6）獲得回饋。

（7）對所聽到的和所看到的作出回應。

（十二）顧客對於資訊安全的期望

資訊安全長計畫過程中的一個重要部分是在確認和討論對於顧客期望的資訊安全。資訊安全過程應該積極地支援機構的商業活動，確保顧客的成就信任和接受機構的安全認證和可信賴供給者是重要考慮。為了採取這個過程應該完成下面的步驟:。

1.確定資訊安全保護措施

2.確定顧客期望

3.確定如何碰到顧客期望

4.確定如何執行矯正計畫

5.確定如何把成就通知給顧客

6.獲得回饋

7.聽和對顧客景觀作出回應

三、擷取必要的諮商與輔導

資訊安全長需要能擷取到一系列資訊安全諮商和輔導，來幫助與保護機構的資訊資源。這些工具應該符合 ISO17799 與 BS7799 驗證，可用來增進機構的使用安全。本章節含有容納應該成為支援工具的一個建議目錄，要理解與聯繫增加的危險資訊安全。

（一）資訊安全長必備的參考工具

參考工具幫助資訊安全長最實用和現實的諮商和原輔導來準備好資訊通路，和對潛在資訊安全事變做相對有效的防禦。而這些工具應該對資訊安全長 ：

1.徹底理解資訊安全。

2.確定資訊資源的概念。

3.建議高級管理階層和董事會, 如何做好資訊安全並風險評估。

4.滿足機構的需要。

5.確定資訊安全威脅和防禦。

（二）建立資訊安全策略樣板的概念

徹底理解所有組織資訊安全的要求，建立一個清楚的資訊安全策略框架，最好是能夠使資訊安全威脅在一個範圍內減到最少。策略應該符合 ISO17799 和 BS7799 國際資訊安全標準。策略樣板可用含有或滿足應付所有機構的專門需要的政策綱領的完全範圍。

（三）對資訊使用者的線上輔導

任何組織內最大的資訊安全風險來源是它自己的雇員，這是一個普遍被接受的事實。但是這些雇員也為防止資訊安全危險，提供一些主要解決方法與工具。如何轉變這些潛在性高的風險來源成為機構的主要防禦，這由組織內部導入一個資訊安全意識文化來完成。這樣的一個環境需要:

1.教育所有雇員資訊安全概念及相關問題。

2.使所有雇員意識到資訊安全威脅和保護措施。

3.幫助雇員在機構裡面認識安全事件的潛在影響。

透過它可容易完成對現行的資訊安全服務，還有產品的執行。經由線上支援系統可以理解資訊安全政策的綱領，作為與

專業的商業活動相關的諮商和輔導。

（四）提供線上使用者資訊和教育的資訊

努力協助資訊使用者在發生問題之前做好資訊保存。資訊安全長要盡力建全資訊安全的策略和方針，補救使用者所發生的錯誤。因此，可以推薦所有使用者資訊和教育的工具，並且可以在線上系統持續提醒使用者保持安全警戒。

第二節 電子商務風險與管理架構

◎具體建議：短程第二項

成立電子商務風險管理服務中心：

- 經濟部主辦，財政部協辦。

有關電子商務發展的問題及政策，臺灣為一個發展中的國家，正在致力於資訊技術的應用，高度重視「知識經濟」將會帶來機遇和挑戰。

臺灣電子商務的發展，既面臨國際共同的法律、稅收、安全等問題，同時受制於電子商務所需的資訊基礎設施問題。完善的電子商務對資訊網路的頻寬速度的要求較高，並需要多媒體支持。然而，在我國高速多媒體頻寬通訊的建設尚未完善成熟，因此，仍需繼續努力。

在臺灣發展電子商務的政策方面, 經濟部長林信義於 89 年 9 月發表一項有關於我國經濟政策方向的演講，其中指出發展臺灣成為「綠色矽島」是我們的目標, 而在以「知識」為主導的新經濟發展潮流中，應用知識和資訊促進新興產業發展，並協助傳統產業調整轉型，則是我們經濟政策的重點。未來經濟部將配合知識經濟方案，做好建構網際網路應用之基礎環境，擴展資訊科技及網際網路在生產及生活上之運用，以及制定電子商務法令等基本工作。

一、建構網際網路應用之基礎環境：

未來將規劃整合型計畫，以便實體配送與虛擬交易環境相互配合，以健全全球運籌的運作體系，擴展資訊科技及網際網路在生產及生活上之運用。經濟部除將積極推動「產業自動化及電子化推動方案」，加速完成產業供應鏈建構外，並加強輔導傳統產業及中小企業對資訊科技之運用，及鼓勵產業技術研究機構增建。

二、制訂電子商務法令等基本工作：

經濟部已經推動電子簽章法立法、宣導正確電子簽章法律觀念，並儘速制定與電子商務有關之資訊安全相關國家標準。

建議成立電子商務風險管理中心，提供下列三點主要的服務，為短程的第二項計畫：

一、提供優良商店標章服務

電子商務風險管理中心對於想獲得優良電子商店標章的電子商店，只要該電子商店對電子商務風險管理中心提出申請，電子商務風險管理中心就會幫助該電子商店規劃設計，使其能夠通過評鑑機構所需評鑑的各個審查項目(欲獲得標章所需達到的標準)，使得該電子商店能夠達到優良電子商店標章安全水準，夠資格取得優良電子商店標章。（優良商店作業的規範請參考：http://www.gsp.org.tw/）

二、提供電子商務風險管理的服務

電子商務風險管理中心能夠對電子商務做以下的評估及服務：

- 網路弱點的評估。
- 掃描電子商店在網路操作上安全的弱點。
- 基本風險的評估。
- 第一者損失和第三者的責任風險的評估。

- 生命週期損失控制的服務。
- 指示電子商店如何建立自己的網路安全和電子商務損失控制機制。
- 訂購損失控制的服務。
- 附加的技術服務，可以幫助電子商店取得或者維持一個安全的電子商務構。

三、代理電子商務保險的事宜

電子商務風險管理中心能夠幫助電子商店代辦電子商務保險，包括電子商務保險的內容及諮詢。使得電子商店能夠透過電子商務風險管理中心的服務，對於適當的項目投保電子商務險，其中包括第一者損失險及第三者責任險。

（一）第一者損失險：

1. 電子資產的損失
2. 個人及廣告的損失
3. 資訊財產的損失

（二）第三者責任險：

1. 電腦欺騙
2. 損壞數位財產
3. 商業收入及額外支出

萬一不幸發生損失或者破壞的時候，也能從電子商務保險取回部分的補償，對於電子商店或者是消費者都會有所保障。透過保險機制的運用，減輕或者是分散消費者及電子商店的責任。有關電子商務風險管理中心服務項目範例可以參考：http://www.insuretrust.com/insurance.html

其中我們以 EXPRESStrust Insurance Policy 代理電子商務保險服務為例子。

保單樣本：

http://www.insuretrust.com/pdfs/EXPRESStrust_specimen.pdf

保險項目摘要：
http://www.insuretrust.com/pdfs/EXPRESStrust_summary.pdf

保單申請書：
http://www.insuretrust.com/pdfs/EXPRESStrust_application.pdf

電子商務係以網際網路通路之虛擬商店與網路銀行（虛擬銀行）風險管理雷同，根據各銀行 89 年 12 月份經由 SET 機制付款閘道之網路轉帳交易量，計有 53,292 筆 ，金額 576,522 千元，平均每筆 10,818 元，而依據資策會統計資料，國內上網人口至 89 年 12 月底已達 550 萬人。因此，估算電子商務成熟時，上網交易人流眾多，約網路銀行之 100 倍，即所可能面臨的風險更大更為複雜，是可以預見的。但就風險分析，其風險類型應相同，如下四類型：

（1）網路交易風險

（2）訊息傳輸風險

（3）業務營運風險

（4）法規遵循風險

而風險管理參照中央銀行金融業務檢查處，89 年 12 月 11 日台央檢任字第 06005060 之號函的要求重點，有下列三方面安全控管：

（1）資訊系統建置方面

（2）內部控制制度方面

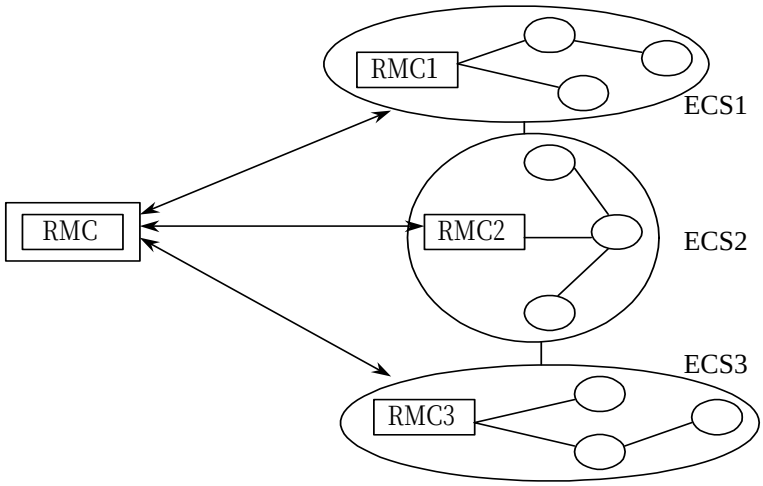
（3）作業程序規範方面

因此，本研究亦將朝這三方面建構風險管理措施，並根據可行電子商務風險與管理之政策與制度模式，設計電子商務風險與管理系統模型。

利用危機預防與偵測觀念，結合風險管理的理論，發展一套電子商務網站風險管理資訊系統架構，建置風險認證，風險估計，風險管理策略規劃，及其安全管理機制評估四大模組，設計網站安全風險管理雛形系統，透過對指標性電子商務網站模擬與分析作業，掌握、防範與處理電子商務網路之安全風險管理，據以編制電子商務風險管理評量表，及推算電子商務管理之平衡評量表，供金融業實行電子商業保險作業的參考，再根據網路資訊安基礎架構管理之原則，具體建議健全我國電子商務風險管理制度。

建置電子商務風險管理中心架構及整體電子商務認證組識架構圖，如圖 8-2 及 8-3 所示：

圖 8- 2 電子商務風險管理中心架構



風險管理伺服中心

- RMSC：Risk Manager Servert Center

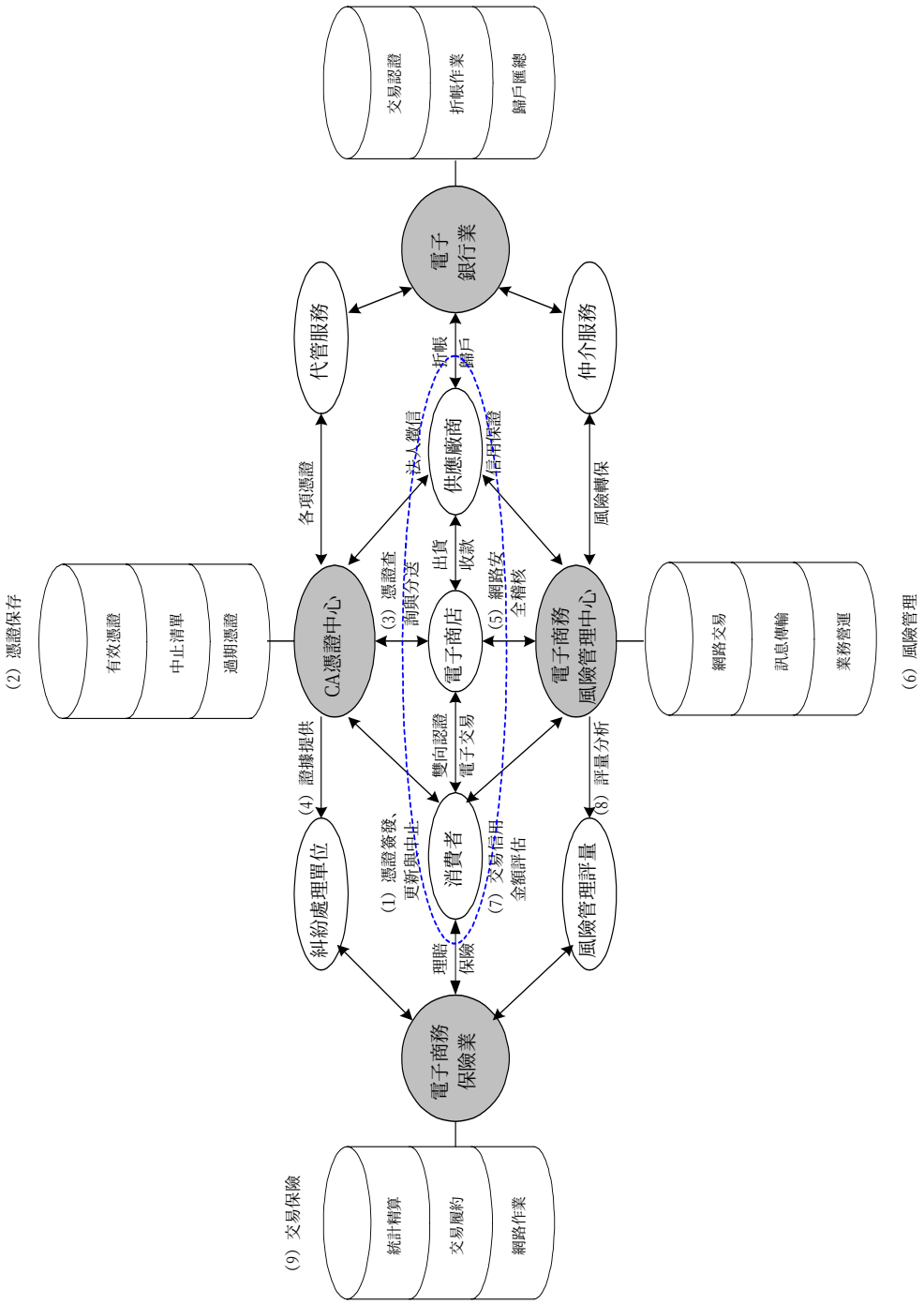
風險管理終端

- RMC：Risk Manager Client/風險管理主管/CRM:Chief Risk Manager

電子商店

- ECS：E-Commerce Shop

圖 8- 3 電子商務驗證組織架構圖



第三節 建立電子商務評鑑及認證組織

◎具體建議：中程

（1）成立電子商務評鑑機構（公正第三者）：

- 經濟部主辦，消基會協辦。

（2）成立電子商務店驗證組織：

- 經濟部主辦，消基會協辦。

（3）推動電子商務保險機制：

- 經濟部、財政部主辦，消基會協辦。

為了確保電子商務風險管理中心能有效管理及服務，本計畫建議由政府核定一個公正的電子商務評鑑機構，該機構對欲申請優良商店標章的電子商店進行各項標章的評鑑，在評鑑合格之後，電子商務評鑑機構將授予該電子商店優良商店之標章，評鑑為優良商店，以取得消費者的信任。而電子商務風險管理中心負責提供欲申請優良商店標章的電子商店相關的服務。例如幫助該電子商店規劃設計，以符合優良商店標章的內容，順利通過電子商務評鑑機構的評鑑，取得優良電子商店的標章。

一、電子商務評鑑機構

評鑑機構為政府監理機構認可之合法的公正第三者，其以客觀公正的立場，對於電子商店給予優良商店標章，電子商務軟、硬體方面的資訊安全，可由業者或公（協）會制定資訊安全準則，並交由此機構來定期抽查，不合格者予限期內改善，合格者發予優良商店標章，其提供的服務如下：

（一） 提供驗證相關的資訊

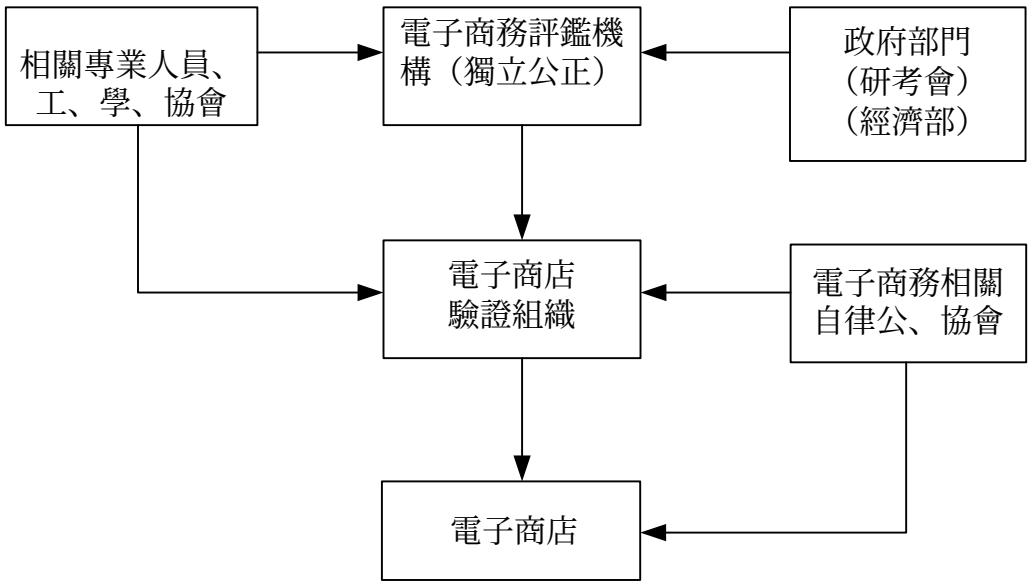
（二） 輔導驗證相關的教育

（三） 辦理驗證審查人員資格考試及證書核發

（四） 驗證審查人員考試內容題庫的建立及維護

國內現階段電子商店驗證市場尚處於發展初期，為有效發揮驗證機制，以及為網路交易建置安全、隱私與公平之電子消費及永續經營環境，政府宜有適當且最基本之管理措施以輔導驗證業者。因此，建議推行驗證活動之基本架構，如圖 8-4 所示：

圖 8- 4 電子商務評鑑組織架構圖



二、電子商店驗證組織：

優良商店作業規範（GSP）認證活動主要目的是要建立一個高品質的商業服務環境，藉由認證活動給予商店業者肯定，強化商店的經營體質，提升服務人員的素質與服務技能，及注意環境安全衛生的內外設備要求，讓顧客要有「安心」、「信賴」、「滿意」服務，同時帶動業者朝向「環境好」、「衛生好」、「制度好」、「服務好」、「經營好」的五好理念努力，以提昇商業服務品質，促進商業現代化。推動 GSP 認證制度的中心思想是：(1) 選訂業種以分期分業認證方式實施，由商店業者自願性參加認證。(2) 通過 GSP 認證之商店獲表揚並授權使用證明標章。(3) 結合相關團體從事廣宣活動，建立消費者對優良商店的信賴，及提高業者對認

證的參與度。

優良商店驗證組織應依下列之四大審查標準，及十二大審查項目定為驗證電子商店的標準，至於細部的審查項目可依電子商店所提出申請驗證之範圍，自行訂定，而本研究報告所提供的細部審查項目如表 8-2 所示，驗證組織可參考訂定之。

表 8- 2 驗證組織審查標準及項目

三大審查標準	十二大審查項目
公司營運策略揭露原則	產品資訊揭露政策 客戶服務及申訴政策 公司政策揭露及網站使用政策
交易完整性原則	交易作業處理政策 付款作業處理政策 物流處理政策
資訊與系統安全原則	隱私權政策 資訊保護 系統安全政策 兒童資訊保護的措施
風險管理與保險機制	永續經營策略 風險管理措施及保險機制應用

三、推動電子商務保險機制

電子商務保險是電子商務風險交易最好的機制。電子商務保險是在保護電子商務交易的雙方，包括電子商店和消費者，因電子商務交易可能會造成財產損失或是責任增加，如果能夠透過保

險機制的運用，則可以減輕或者分散消費者和電子商店的風險，即應可以電子商務風險保險聯盟組織來運作。

風險管理包括確定、評估與管理三大步驟，風險包括人事、需求、技術、商業等複雜的組合。找出可能的潛在風險，就是風險管理的第一步。風險評估要評估電子商務與企業 e 化的風險十分困難。一般來說，可藉由顧問或有經驗的人獲得，定期評估可以有效防止潛在風險，而不會等到事態嚴重的時候才發現。預防風險最好的方法就是妥善的準備，定期地評估、溝通與改善，也是降低風險的不二法門，而有效的知識管理策略更是預防風險的利器。

第四節 電子商務永續經營計畫

◎具體建議：長程

（1） **建議電子商務風險管理中心及保險機制，納入國家資訊基礎建設範疇：**

- 經濟部、財政部主辦，交通部協辦。

（2） **促成電子商務風險管理中心以國家組織的方式積極參與 CIS (the center for Internet service) 為國際性非營私公司組織 (cooperative organization)標章服務工作 (charter service) ：**

- 經濟部主辦，外交部、消基會協辦。

一、建立電子商務風險管理中心及保險機制為國家資訊基礎建設的範疇

建立電子商務風險管理中心的目的是在服務電子商店，使得消費者對電子商務更有信心，增強消費者利用網路來消費的便利性。對於幫助電子商店成為優良電子商店的目標如下：

（一）提升電子商店服務品質經營水準：

針對各業種業態服務人員，進行服務技巧專業訓練，並進一步導入企業內應用，藉以提升商業整體服務技能、服務水準，強化經營競爭力。

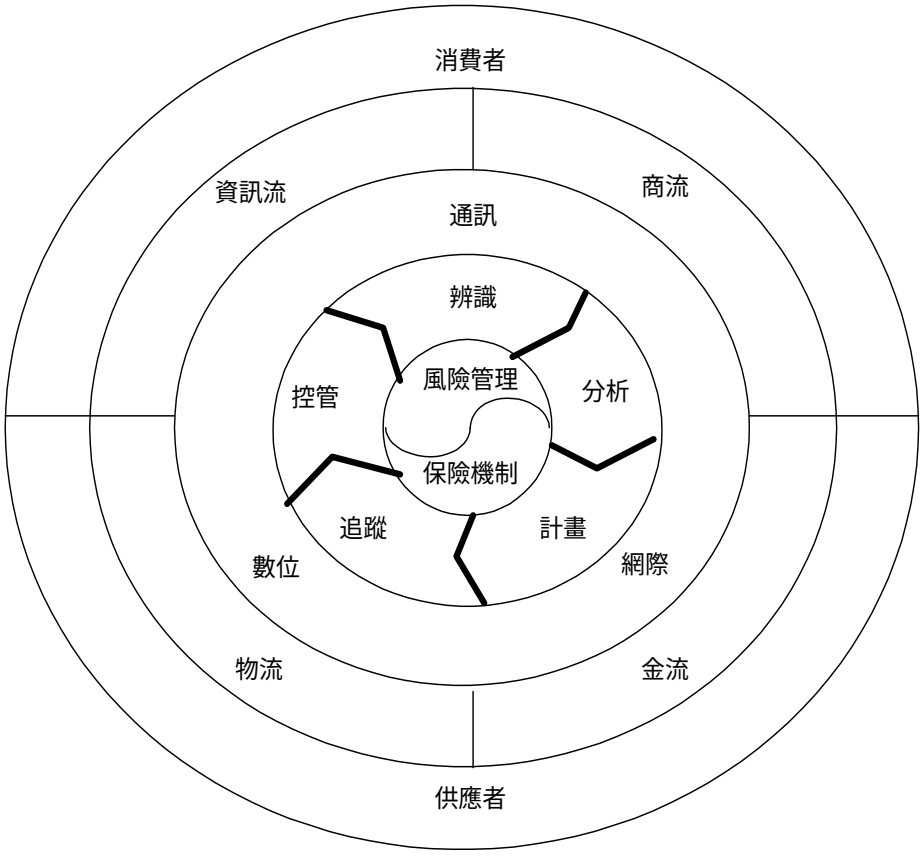
（二）強化電子商店服務品質意識：

與 ISO 精神結合，以利內部品質稽核觀念與精神真正落實於企業內部管理中，達到國際共同規範。

（三）塑造電子商店全面顧客滿意新形象：

結合多方面力量，擴大優良商店（GSP）作業規範認證標章之認知度及知名度，讓社會大眾能清晰、簡單的認識優良商店之優點，塑造商業服務業全面顧客滿意新形象。

圖 8- 5 電子商務風險管理與保險機制示意圖



此外電子商務風險管理中心也具有電子商務風險管理的服務。且幫助電子商店投保電子商務險，圖 8-5 為電子商務風險管理與保險機制示意圖。使得經過電子商務風險管理中心協助過的電子商店能夠贏得顧客的安心、信賴及滿意。建立成為一個環境好、衛生好、制度好、服務好、經營好的電子商店。

二、積極參與國際性非營私公司組織為標章服務工作

（一）規劃建置一個危機恢復程序：

指定 BCP(business continuity planning)商業連續性計畫作業對企業的責任。運用一個好的運作及特定的計畫管理來衡量審查資訊安全。對這種情勢有三個很重要的技巧：商業操作的知識、良好的溝通、計畫的管理。

引導風險分析決定於企業產品設備毀壞之後，恢復業務操作的能力。中間的分析報告將提供：恢復計畫在現行的業務運作之下在哪裡沒有做好。假如企業沒有危機管理的團隊，那麼就建立一個危機管理的團隊。建立一個危機決策等級去分類一些實行時不可得知的潛在因素，制定企業在處理危機事件時的規則及更新的步驟，設計多種可行的恢復程序對於對外的溝通、股東、工業分析師、主要客戶、內部員工、生意夥伴。

定期更新員工聯絡和溝通的管道。例如：住家、辦公室、行動電話、渡假處的電話號碼、攜帶型傳呼機號碼、辦公室及個人電子信箱地址。如果在公司發生事情時能夠自動通知。建立追蹤員工下落的程序，使得公司在正常營運的時候，員工的去向都能在公司掌控之內。平時也要教育員工潛在的災難預防，訓練員工對於事件發生時的反應，包緊急疏散和聯絡的程序。

決定哪些通訊方法是可行的，建立主要的通訊方式。電子郵件、即時訊息都能給員工作為通訊使用。至於個人通報系統則要使用有限距離的通訊方式，例如對線上的員工或者身旁的員工，就安裝免費的電話號碼給員工和他們喜歡的人，讓他們

能接收訊息和散佈資訊。如果災難發生時，則安排臨時的辦公空間使用。雖然災難回復系統的提供者可以在災害發生時提供辦公空間和設備給非會員的顧客，但是他們無法提供相似的恢復服務給企業 IT 設備。觀察企業額外的支出和商業保險政策，以確保他們包含現行商業運作情形是安全的。

觀察備份和儲存的策略，以確保全部的資訊流是安全的，包括應用、連線和存取點能夠被恢復。而且備份的資訊能夠很容易的被恢復，且帶去交替恢復的網站。每個部門必須的設備：手電筒、毯子、緊急事件聯絡裝置、水、不易腐壞的食物、醫藥提供。

（二）為特定的災難種類做計畫準備：

1. 確保事態說明計畫的過程和恢復對業務運作是安全的，除了對自然災禍和自然力量的傳統情形的說明以外還要包括火災和電訊的停擺。
2. 發展連續性計畫必須包括主要供應者停擺時的應變措施，例如：策略聯盟，外部服務供應者，公共建設的服務(例如：郵件和電話)或者通訊服務。必須要確保即使一個事件對企業產生了衝擊，但是企業的業務操作仍然能繼續運作。
3. 回顧所有業務運作時外部服務供應者的業務連續性計畫，企業用來確保他們的計畫安全。確保與這樣的供應商所簽的企業業務連續性的合約會是安全的。
4. 制定人員援助模式，提供醫療援助和其他的服務。
5. 保持在一個短時間之內能夠提供目前供應商合約人員的流程表(例如：12 到 24 小時)與企業的需要相匹配的技術，尤其是 IT 技術裝置。
6. 以適當的配置位置，提供人員的佈署(例如：足夠的辦公空間、電話和電腦傳真機和其他的辦公室設備) 。
7. 由於在恢復情況的期間，人員工作時間太久。注意員工的需

要，確保食物的品質和多樣化，和在輪流辦公的場所提供休息和有形的活動設備。

8. 企業必須成立其他的根據地，以供緊急事件發生時還有代辦處可以運作，確保企業能夠從事件衝擊中恢復過來。給這些當權和代理人接觸的資訊，可以包含在業務連續性計畫裡，如果適當可以把他們包括在災禍恢復測試裡。

9. 確保能夠恢復對部門和分散的工作地區，對網路核心關聯點的服務。

10.確保企業只能用紙紀錄的關鍵性重要記錄的備份，隨著此時有效傳輸可獲得的位置存儲。

（三）實施長期的 BCP 作業：

制定一個業務連續性計畫，包括商業和技術性的操作。

1.建立 BCP 到 IT 計劃的生命週期，人類資源變化的過程(保持人員接觸尤其重要)，設備和組織的改變。

2.制定一個管理連續性的計畫以提出一些實施時也許難以獲得的潛在因素。

3.年長的高級管理者對彼此的支援，使得整個團隊沒有因為災禍而迷失。

4.回顧高級管理者的策略，關鍵的實行不應該一起實行。

5.如果可能，不同的地方的人員，不可以被一個缺少資歷的 職員阻止恢復的過程。

6.把遠距離工作看作對一些人員的選擇。如果企業已經支援遠距離工作，就應該在災禍期間依照路程途徑優先決定誰將收到通知。

7.把閒置不用的資料中心與使用的職員資源分離，因此即使損壞這個資料中心，人員保留的資料仍然是可用的。

8.重複和實行所有業務連續性計畫的測驗，在業務操作和恢復的能力之間找到可能的空隙。

（四）維護 BCP 的資訊安全：

在業務連續性計畫中含有的資訊，關於企業與員工的秘密和高敏感度的資訊。個人電話號碼，電子郵件並且提出必須保護其他接觸資訊，以確保沒有違反秘密或者秘密的規則破壞。應該把涉及在業務連續性計畫方面的業務程序看作企業的智力性質，並且他們應該被保護。

1.內部人員接觸的名單應該限制分發。

2.Call trees 只需要有接觸資訊，不需要個人的地址。

3.業務連續性計畫可能切割每一個他們執行負責的恢復部門變成全部計畫的一部分。

（五）永續經營管理政策

電子商務的經營，為了能夠不斷的獲利，不斷的營運。經營者必須有永續經營的觀念。對於永續經營觀念的實行，我們提出了以下的策略，以供電子商務經營者能將之應用在其電子商務網站中，達到電子商務永續經營的目標。

細部審查之項目：

1. 建立網路品牌

2. 贏得顧客信賴

3. 登錄各大搜尋引擎

4. 安全付款機制

5. 互動式網站

6. 相關網站連結

7. 客服中心

8. 追蹤客源

9. 利用電子郵件行銷

10. 利用電子報

11. 獎勵機制

永續經營控制的重點如下：

1. 電子商務網站設計

2. 網站店面設計

3. 網站服務設計

4. 網站商務促銷設計

（六）政府對災禍恢復應採取的步驟：

1. 與各級的政府部門保持通訊的暢通，資訊應該透過不同的管道公佈(例如：印刷媒介、無線電和電視、網際網路之間)。

2. 用這些相同的通道，來提供關於解決緊急事件計畫的細節資訊和命令。

3. 確保所有政府雇員在災禍恢復的工作上都能迅速簡捷，且保持每日上傳災禍與恢復的努力成果。公眾的信任來自政府雇員，這提供精確的資訊和防止沒有根據的資訊傳播，使他們成為一個極好資源。

4. 設備、服務和業務的槓桿作用關係。

例如：政府為緩解交通經常增加大型車輛，例如貨車、公共汽車、 貨車和各種類型的大型車輛。

（七）對於災禍恢復政府未來應做的對策

在計畫和恢復期間，有哪些必須由經營管理者那裡得到支援。這是將來業務連續性計畫制定者所必須準備的，這個支援連續性計畫基本上將保留次要關心的事--風險的文件--，並且政

府很可能不能從災禍中恢復過來，為了得到支持他們的努力，業務連續性計畫制定者應該要有些防範措施。

附錄(一) 期末報告初稿學者專家座談會會議紀錄

一、時間：九十一年三月十一日（一）上午九時三十分

二、地點：本會七樓簡報室

三、主席：林主任委員嘉誠
紀錄：陳佳君

四、出（列）席人員：

- ✧ 學者專家（依姓氏筆劃排列）：
- ✧ 江教授炯聰（台灣大學工商管理學系）
- ✧ 沈司長臨龍（財政部保險司；王科長桂春代）
- ✧ 林董事長世華（中華民國網路消費協會）
- ✧ 吳總經理啟昌（文佳科技股份有限公司）
- ✧ 曹教授承礎（台灣大學資訊管理學系）
- ✧ 劉司長坤堂（經濟部商業司；未出席，提供書面意見）
- ✧ 葛執行長亦愚（財團法人中華民國國家資訊基本建設產業發展協進會）
- ✧ 藍副總經理敏宗（宏遠育成科技股份有限公司）
- ✧ 龔主任仁文（財團法人資訊工業策進會電子商務推廣應用中心；林世懿小姐代）

研究小組成員：

- ✧ 趙教授健明（財團法人成大研究發展基金會）
- ✧ 葉俊麟先生（研究助理）
- ✧ 張榮庭先生（研究助理）

本會列席人員：

- ✧ 楊處長秀娟
- ✧ 林高級分析師裕權
- ✧ 黃科長忠真
- ✧ 吳副研究員文峰

五、主席致詞：(略)

六、研究小組報告：(略)

七、發言要點：(依發言順序)

(一) 江教授炯聰（台灣大學工商管理學系)：

1、對電子商務相關議題的整理較有系統，但對風險管理的因果研究不深入。

2、相關資料蒐集豐富，但有關法制方面相當不足。

3、對於研究目的有基本問題認知之貢獻，但對於可行性作法欠缺足夠之論證。

4、建議加強風險管理機制之研究，嘗試應用在電子商務領域討論其類型，以把握適當機制之限制運用範圍與互補功能。特別是有關市場機制、立法行政機制、與法院機制在效率及公平正義原則下的運作，在嚇阻、誘因與損害分散等面向之考量。

（二）曹教授承礎（台灣大學資訊管理學系)：

1、針對具體建議之導出，相對之研究方法可分析現有或潛在之因素，擬定本研究所提建議之定位。

2、各建議事項應探討其背景、目的、作法與現今國內外作法之比較、與傳統經營方式之比較、經費、人員等各項因素之搭配，再進行可行性分析。

3、建議事項之短、中、長程優先順序、重要性之擬定應有其依據，才能做為本研究之主要參考。

（三）林董事長世華（中華民國網路消費協會）：

1、研究發現中似可加入消費者的風險，如消費者申訴機制的欠缺，導致消費者申訴不如實體商店之效率，是否有必要設置標準內容網站，讓電子商務網站具備基本要素（如交易確認、申訴機制、交易查詢等）。

2、OECD 電子商務消費者保護綱領列有 B2B 網站建置要件，行政院消費者保護委員會亦訂有「電子商務消費者保護綱領」，國內 B2B 網站如何導引至該標準（定型化網站），政府可委外設計，提供業界使用，並依企業個別需求，授權由業者依各自需求量身訂作。

3、網路市集或網路商場方面，宜補助業者以商業化方式建立保險信託機制，此種信賴機制宜由具公信力之消費者團體出具。

4、研究建議中提及由消基會協辦成立電子商務驗證組織及保險機制部分，與消基會的宗旨不符，且易導致消費者過度信賴及廣告誤導，徒增糾紛之機率。

5、保險及標章之差異中，保險係商品，應順應商業需求並誘導其發展；標章部分若以法規方式引導使用，可有效將紊亂無章的標誌導引至消費者易於辨識、易於宣導的信賴標誌。

6、以法規導引是最簡易的推動方法，既然電子商務的風險如此高，消費者保障是很需要的，強制要求一定流量以上的交易網站（例如遊戲網站）應使用定型化網站及標誌。

（四）葛執行長亦愚（財團法人中華民國國家資訊基本建設產業發展協進會）：

1、資訊安全與風險管理的機制，依據企業或組織的大小有其程度性差異希望在研究報告內能作更進一步的區分，例如哪些項目是哪種規模的企業或組織必備的，哪些是選擇性的具備

即可。

2、相關性電子商務安全組織及風險管理服務中心的組織架構，建議依據企業或組織規格的大小或可能實際的需求作成分級，較能有效地達成實際效果。

3。報告部分內容係由國外的資訊轉錄而來，因而在描述方面有重覆的地方。如第三章說明電子商務產業領域風險的介紹時，建議先作共通性的風險描述後，再按領域作個別性風險的描述，增加報告可讀性。

4、研究建議事項於執行時應結合電子商務實務上的進度，方能更為有效。

（五）林世懿小姐（財團法人資訊工業策進會電子商務推廣應用中心）：

1、研究架構不清晰，導致章節關聯性不易看出。

2、文獻探討部分與研究建議關聯性薄弱，不易支持論證及建議，且國外相關制度的探討較欠缺。

3、電子商務保險機制由政府介入的適合性須再探討。

（六）王科長桂春（財政部保險司）：

1、財政部九十年九月十九日以台財保第０九００七五一００四號函核准蘇黎世電子商務綜合保險，雖已逾半年，然據該保險公司表示，雖然積極洽攬業務，惟目前仍未銷售出單，並稱因國內業者對電子網路行銷大多仍屬輔助階段，因此對整體營業收入（中斷）影響不大，是以購買意願不高。

2、報告提要中，對於健全我國電子商務風險管理制度之具體建議表中程（３）：推動電子商務保險機制由經濟部及財政部主辦，似有不宜，財政部業已核准電子商務綜合保險產品，業者若有需求，當可逕洽保險公司辦理；另考量電子商務牽涉範圍甚大，風險性極大，保險公司是否承保，亦須端賴國外

再保公司之意願，因此該業務推動是否宜由財政部主導，宜請研究小組再研酌。

3、長程計畫建議電子商務風險管理中心及保險機制納入國家資訊基礎建設範疇，由經濟部及財政部主辦乙節，由於該管理中心規劃負有代辦電子商務保險事宜及該保險內容之諮詢，與現行保險法令似有不合，宜請研究小組再加研酌。

4、網路安全政策之落實、公司內部電腦稽核制度之健全、外部電腦稽核工作之強化，均為電子商務損害防阻之重要環節，亦可降底保戶之保險費負擔。

5、研究小組對保險方面若有任何問題，可洽本部保險司辦理。會後若提供國外電子商務保險保單資料，本部自當研究參辦。

（七）吳總經理啟昌（文佳科技股份有限公司）：

1、針對 B2B 及 B2C 的不同風險管理進行分類、分析，先確立風險在哪裏後再來談保險。

2、研究資料宜對國內相關單位的制度、規章多加蒐集並加以整合及討論。

3、研究建議應考量民間及各國企業實行的比較。

4、短程建議希望以研考會為主，研究出一個較為符合台灣活力的方式。

5、研究報告修正時請詳校錯漏字。

（八）藍副總經理敏宗（宏遠育成科技股份有限公司）：

1、五十一頁至六十一頁有關實體風險（如火災）不須著墨太多。

2、研究報告應加強電子處理過程所可能發生的犯罪及建議防止機制，包括犯罪者紀錄資料庫，以列為拒絕往來戶，嚇阻犯罪意圖。同時犯罪者紀錄不應只記錄公司名稱，應記錄公司所有上層主管，預防另開公司詐騙。

3、研究資料可增加電子世界領域的犯罪例子及防止方法。

4、研究建議成立風險管理中心、評鑑機構、商店驗證組織等，有疊床架屋之嫌，應納入同一組織即可。且本案宜對網路安全機制繼續深入研究，暫勿急於成立組織。

5、研究報告中、英文文字請修訂校正，以求精簡、正確。

（九）劉司長坤堂（經濟部商業司；未出席，提供書面意見）：

1、研究資料建議補充電子商務保險制度在亞太地區方面的情況、各國電子商務風險管理制度、電子商務保險市場規模及目前保險業者所提供之電子商務保險險種之相關資料，以供參考。

2、建議針對電子商務軟、硬體方面的資訊安全，是否可由業者或公（協）會制定資訊安全準則，並交由專責機構定期抽查，不合格者予限期內改善，合格者發予優良商店標章，以取代電子商務風險管理服務中心進行可行性研究。

3、在電子簽章法通過後，確立了電子簽章之法律效力，但目前B2C電子商務除了網路銀行及網路證券交易採SET及電子簽章外，多數交易在不可否認性上仍有疑義。在此情況下，保險制度在責任歸屬上有重大困難度。要推動電子商務保險機制應先解決此問題。

4、建議增加各國電子商務風險管理制度比較之章節。

（十）本會意見：

1、研究發現並未依本會專案作業要點規定專章論述，僅於提要中說明。且研究發現敘述上似顯薄弱不足，宜加以進一步詳細說明。

2、各建議事項提出風險管理環境建置與機制，並以表列方式說明各項內容，惟多屬功能性之說明，缺乏法制面建構之規劃意見。

3、對於如何有效管理電子商務風險，宜加強政府在健全相關制度環境，如法令規章研修等之相關建議，並應加強民間參與的策略規劃，俾能有利於工作推動的加強與落實，較不宜採「大有為政府」的策略。

4、在政府機關資訊安全組織規劃上，應非僅關設置資訊安全長，宜進一步對整體組織調配，考量可行性，研提較具體的建議，例如有關電腦緊急事件通報處理機制、資訊安全稽核制度的規劃建議等。

5、有關 Micro Payment 的機制若能建立，應可有效減低網路付款的風險，建議可加強相關內容。

6、報告第一章、第二章、第四章第二節及第六章第三節文字敘述似由原文直接翻譯，未加潤飾，使得文章敘述語句片斷呈現，無法組成完整語句，不易閱讀理解。

7、本研究案希望透過國外電子商務風險管理措施（如電腦稽核、簽章認證等）及實施經驗，以及國內目前電子商務管理情形，瞭解電子商務的可行管理措施。報告中對於國內外風險管理措施相關資料豐富，但對國內外實施經驗及案例分析則較少著墨。

8、封面、章節標記及版面配置，部分未依本會專案研究作業要點規定格式。

9、報告中部分用詞請統一，如「提昇」或「提升」、「　謗」或「誹謗」、「違反」或「違犯」、「收集」或「搜集」等，錯漏字請再詳校更正。

八、研究小組說明：

這是我們第一次投入電子商務的研究中，但有些技術層面的問題待克服。我們目前也在編資通安全作業手冊，對 ISO17799 相關電子商務安全資料都看的很仔細。對政府有此雄心，想要讓消費者可以安心地在電子商店採購，如同林董事長所說的，所有

的消費者到台灣的電子商店購物都可以得到二００元的保險保證，那台灣的電子商務一定是全世界第一名的。

九、主席結論：

（一）謝謝趙教授和他的研究團隊，也謝謝三位評審委員參與整個研究案研究重點的設計規劃。電子商務是個相當大的議題, 也是跨國際的問題, 本研究案主要針對 B2C 進行討論, 目前國內的狀況在報告中列有相關網站供參考。

（二）本會在委外研究時，大都希望研究小組提出具體的建議，若委託研究是屬於比較前瞻性，將會在下一個階段做更具體的研究，不會馬上列為政策要求執行。

（三）行政及政策類的委託研究與一般的學術委託不同，希望彙集產、官、學三方面的意見，有一個比較具體的方向，提供執行單位或規劃、審核計畫時參考。今天在座各位提供的意見，將有助於我們面對二十一世紀的 e-society。這篇報告請趙教授依據大家的建議修改，再度感謝各位參加今天的座談會。

十、散會（上午十一時）

附錄（二）專家座談意見本研究小組修正紀錄表

一、江教授炯聰
（一）對電子商務相關議題的整理較有系統，但對風險管理的因果研究不深入。 （二）相關資料蒐集豐富，但有關法制方面相當不足。 （三）對於研究目的有基本問題認知之貢獻，但對於可行性作法欠缺足夠之論證。 （四）建議加強風險管理機制之研究，嘗試應用在電子商務領域討論其類型，以把握適當機制之限制運用範圍與互補功能。特別是有關市場機制、立法行政機制、與法院機制在效率及公平正義原則下的運作，在嚇阻、誘因與損害分散等面向之考量。
研究小組修正紀錄之一
（一）本研究小組已根據江教授之建議，修改了部分內容，請參考第五章之內文。 （二）由於國內電子商務仍在起步階段，所以在立法方面的資訊不夠充分，在本報告第五章第一節中有介紹各國電子商務立法的現狀，可供國內參考。 （三）本研究小組所研究之報告，是經由篩選國內外相關電子商務推行成果及經驗，所以應該有足夠的論證，對於相關電子商務風險管理的政策，可參考第五章第三節。 （四）本研究小組已經在第五章第三節和第四節中增修風險管理的研究。在電子商務的推動上，對於市場機制、立法行政機制與法院機制，確實應該在有效率及公平正義的原則下運作進行，此項建議將轉送政府相關單位納入行政考量。

二、曹教授承礎
（一）針對具體建議之導出，相對之研究方法可分析現有或潛在之因素，擬定本研究所提建議之定位。 （二）各建議事項應探討其背景、目的、作法與現今國內外作法之比較、與傳統經營方式之比較、經費、人員等各項因素之搭配，再進行可行性分析。 （三）建議事項之短、中、長程優先順序、重要性之擬定應有其依據，才能做為本研究之主要參考。
研究小組修正紀錄之二
（一）本研究小組已將短、中、長程具體建議，於第八章詳述其具體作法。 （二）有關於國內外作法之比較，可見於第五章第一節之內文。本研究小組已將短、中、長程具體建議，於第八章詳述其具體作法。 （三）本研究小組已經在本書中第八章中，增修對於短、中、長程優先順序與重要的評估、探討。
三、林董事長世華
（一）研究發現中似可加入消費者的風險，如消費者申訴機制的欠缺，導致消費者申訴不如實體商店之效率，是否有必要設置標準內容網站，讓電子商務網站具備基本要素（如交易確認、申訴機制、交易查詢等）。 （二）OECD 電子商務消費者保護綱領列有 B2B 網站建置要件，行政院消費者保護委員會亦訂有「電子商務消費者保護綱領」，國內 B2B 網站如何導引至該標準（定型化網站），政府可委外設計，提供業界使用，並依企業個別需求，授權由業者依各自需求量身訂作。

（三）網路市集或網路商場方面，宜補助業者以商業化方式建立保險信託機制，此種信賴機制宜由具公信力之消費者團體出具。 （四）研究建議中提及由消基會協辦成立電子商務驗證組織及保險機制部分，與消基會的宗旨不符，且易導致消費者過度信賴及廣告誤導，徒增糾紛之機率。 （五）保險及標章之差異中，保險係商品，應順應商業需求並誘導其發展；標章部分若以法規方式引導使用，可有效將紊亂無章的標誌導引至消費者易於辨識、易於宣導的信賴標誌。 （六）以法規導引是最簡易的推動方法，既然電子商務的風險如此高，消費者保障是很需要的，強制要求一定流量以上的交易網站（例如遊戲網站）應使用定型化網站及標誌。
研究小組修正紀錄之三
（一）從消費者角度辦理小額交易保險，是一項不錯的建議，可以建立消費者在從事電子交易的信心。財政部保險司應鼓勵業者推動。 （二）此項意見很好，建議政府相關單位在行政時能納入考量。 （三）此項意見很好，正如報告中第七章第二節所提，如何將電子商務保險機制在政府、企業、個人三方面，創造三贏的局面。也希望政府在行政時能納入考量。 （四）電子商務驗證組織及保險機制交由消基會協辦的目的，在於消基會的公信力高，本研究小組覺得好處是可以藉由消基會的公信力高可以幫助推廣電子商務的實行。 （五）關於保險部分，希望保險的機制可以很有彈性，以適應商業的需求。關於標章方面，希望能全部以法規的方式使用。使消費者易於辨識標章且對標章產生信賴，以便推動電子商務的運作。 （六）本研究小組建議採用標章的發行，並請參照本研究第八章第三

節所述，以期能保障消費者及商家之間的權益。
四、葛執行長亦愚
（一）資訊安全與風險管理的機制，依據企業或組織的大小有其程度性差異希望在研究報告內能作更進一步的區分，例如哪些項目是哪種規模的企業或組織必備的，哪些是選擇性的具備即可。 （二）相關性電子商務安全組織及風險管理服務中心的組織架構，建議依據企業或組織規格的大小或可能實際的需求作成分級，較能有效地達成實際效果。 （三）報告部分內容係由國外的資訊轉錄而來，因而在描述方面有重覆的地方。如第三章說明電子商務產業領域風險的介紹時，建議先作共通性的風險描述後，再按領域作個別性風險的描述，增加報告可讀性。 （四）研究建議事項於執行時應結合電子商務實務上的進度，方能更為有效。
研究小組修正紀錄之四
（一）不論企業的規模大小，都應該依據資訊安全與風險管理的機制建立，不過台灣企業規模的差異甚大，並不容易以明確的方式定義出企業規模的大小程度。所以本研究小組建議由電子商務評鑑機構來衡量這些標準。在本書第八章第三節中有提出表 8-2 驗證組織審查標準及項目可供參考。 （二）此項建議（一）建議有相關，可參考本書第八章第三節之內容。 （三）本研究小組已經詳細地校正過報告的內容，將內容重複的地方整合完成。 （四）委員的建議很好，希望政府相關單位在推廣電子商務時能納入行政的考量。

五、林世懿小姐
（一）研究架構不清晰，導致章節關聯性不易看出。 （二）文獻探討部分與研究建議關聯性薄弱，不易支持論證及建議，且國外相關制度的探討較欠缺。 （三）電子商務保險機制由政府介入的適合性須再探討。
研究小組修正紀錄之五
（一）本研究小組已經根據建議，重新調整報告整體的架構。 （二）本研究小組亦尋找了更多的相關資料，並經過討論依其性質特點，加入本書各個章節之中。現在報告已經相當完整，章節的關聯性也有改善。 （三）電子商務保險機制的建立，政府應扮演建立好保險相關的基礎建設的角色，包括法律、資訊、及策略三個層面，並「協助」保險業者開發新產品及電子商務網站承保相關保險，達到與已開發國家相同交易保障的水準。而並非由政府直接辦理保險業務。
六、王科長桂春
（一）財政部九十年九月十九日以台財保第０九００七五一００四號函核准蘇黎世電子商務綜合保險，雖已逾半年，然據該保險公司表示，雖然積極洽攬業務，惟目前仍未銷售出單，並稱因國內業者對電子網路行銷大多仍屬輔助階段，因此對整體營業收入（中斷）影響不大，是以購買意願不高。 （二）報告提要中，對於健全我國電子商務風險管理制度之具體建議表中程（３）：推動電子商務保險機制由經濟部及財政部主辦，似有不宜，財政部業已核准電子商務綜合保險產品，業者若有需求，當可逕洽保險公司辦理；另考量電子商務牽涉範圍甚大，風險性極大，保險公司是否承保，亦須端賴國外再保公司

之意願，因此該業務推動是否宜由財政部主導，宜請研究小組再研酌。

（三）長程計畫建議電子商務風險管理中心及保險機制納入國家資訊基礎建設範疇，由經濟部及財政部主辦乙節，由於該管理中心規劃負有代辦電子商務保險事宜及該保險內容之諮詢，與現行保險法令似有不合，宜請研究小組再加研酌。

（四）網路安全政策之落實、公司內部電腦稽核制度之健全、外部電腦稽核工作之強化，均為電子商務損害防阻之重要環節，亦可降底保戶之保險費負擔。

（五）研究小組對保險方面若有任何問題，可洽本部保險司辦理。會後若提供國外電子商務保險保單資料，本部自當研究參辦。

研究小組修正紀錄之六

（一）就如同王科長所言，因為國內業者電子商務行銷大多在輔助階段，故尚未有熱絡的承保動作。然而財政部於九十年九月份所通過的第一張電子商務保單，也代表著國內電子商務交易機制邁向國際化。未來不管是國內專屬或國際性交易網站，都可以直接在國內保險公司購買相關保險。

（二）感謝委員建議。關於此點，本研究小組會商請相關單位，評估建議方向實行的可能性。

（三）感謝委員建議。關於此點，本研究小組會咨詢相關單位，並於第八章第四節中修正之。

（四）網路安全政策之落實、公司內部電腦稽核制度之健全、外部電腦稽核工作之強化，確為電子商務損害防阻之重要環節，可降底保戶之保險費 負擔，與本文第七章所提之觀念雷同。

（五）感謝王科長熱情相助，本研究小組若有相關保險方面的問題，必當請教貴單位保險司。

七、吳總經理啟昌
（一）針對 B2B 及 B2C 的不同風險管理進行分類、分析，先確立風險在哪裏後再來談保險。 （二）研究資料宜對國內相關單位的制度、規章多加蒐集並加以整合及討論。 （三）研究建議應考量民間及各國企業實行的比較。 （四）短程建議希望以研考會為主，研究出一個較為符合台灣活力的方式。 （五）研究報告修正時請詳校錯漏字。
研究小組修正紀錄之七
（一）感謝委員的建議。有關於電子商務的各類風險在第五章第三節有詳細的介紹，而在談論保險之前也必須先確立風險的起因，方能對電子商務的風險有效的管理。 （二）本研究小組已經根據建議，整合報告內容。 （三）本研究小組已在第五章第一節裡補充我們所不足的地方。 （四）感謝委員的建議。關於此點，本研究小組會考慮這個建議方向，會商相關政府單位。 （五）已修正研究報告之錯漏字。
八、藍副總經理敏宗
（一）五十一頁至六十一頁有關實體風險（如火災）不須著墨太多。 （二）研究報告應加強電子處理過程所可能發生的犯罪及建議防止機制，包括犯罪者紀錄資料庫，以列為拒絕往來戶，嚇阻犯罪意圖。同時犯罪者紀錄不應只記錄公司名稱，應記錄公司所有上層主管，預防另開公司詐騙。

（三）研究資料可增加電子世界領域的犯罪例子及防止方法。

（四）研究建議成立風險管理中心、評鑑機構、商店驗證組織等，有疊床架屋之嫌，應納入同一組織即可。且本案宜對網路安全機制繼續深入研究，暫勿急於成立組織。

（五）研究報告中英文文字請修訂校正，以求精簡、正確。

研究小組修正紀錄之八

（一）已修正研究報告之內容。

（二）此項建議相當有建設性，本研究小組已將其納入第四章第三節的內文之中。

（三）已將此意見納入第四章第三節現行風險管理的機制與架構之檢討的內文中探討。

（四）本研究小組建議分別成立風險管理中心、評鑑機構、商店驗證組織等，是有相互制宜的目的，但若需配合政府組織縮編的政策，在電子商務推動的初期，要納入同一組織亦無不可。另一有關網路安全機制的問題，已於第三章第三節及第五章第三節中列入研究。

（五）在報告中之英文文字已修訂校正。

九、劉司長坤堂

（一）研究資料建議補充電子商務保險制度在亞太地區方面的情況、各國電子商務風險管理制度、電子商務保險市場規模及目前保險業者所提供之電子商務保險險種之相關資料，以供參考。

（二）建議針對電子商務軟、硬體方面的資訊安全，是否可由業者或公（協）會制定資訊安全準則，並交由專責機構定期抽查，不合格者予限期內改善，合格者發予優良商店標章，以取代電子商務風險管理服務中心進行可行性研究。

（三）在電子簽章法通過後，確立了電子簽章之法律效力，但目前B2C電子商務除了網路銀行及網路證券交易採SET及電子簽章外，多數交易在不可否認性上仍有疑義。在此情況下，保險制度在責任歸屬上有重大困難度。要推動電子商務保險機制應先解決此問題。 （四）建議增加各國電子商務風險管理制度比較之章節。
研究小組修正紀錄之九
（一）在第四章第三節中有列出各國電子商務風險的運作情形，於第五章第三節有提及電子商務的管理政策，有關電子商務保險的相關細節，請參考第七章內容，及其所列之參考網站。 （二）已將此建議針納入第八章第三節內容中的電子商務評鑑機構。 （三）此項建議實屬前瞻，已列入第七章之內文之中，以作為政府相關單位之行政參考。 （四）請參考第四章第三節及第五章第三節之介紹。
十、研考會
（一）研究發現並未依本會專案作業要點規定專章論述，僅於提要中說明。且研究發現敘述上似顯薄弱不足，宜加以進一步詳細說明。 （二）各建議事項提出風險管理環境建置與機制，並以表列方式說明各項內容，惟多屬功能性之說明，缺乏法制面建構之規劃意見。 （三）對於如何有效管理電子商務風險，宜加強政府在健全相關制度環境，如法令規章研修等之相關建議，並應加強民間參與的策略規劃，俾能有利於工作推動的加強與落實，較不宜採「大有為政府」的策略。 （四）在政府機關資訊安全組織規劃上，應非僅關設置資訊安全長，宜進一步對整體組織調配，考量可行性，研提較具體的建議，

例如有關電腦緊急事件通報處理機制、資訊安全稽核制度的規劃建議等。

（五）有關 Micro Payment 的機制若能建立，應可有效減低網路付款的風險，建議可加強相關內容。

（六）報告第一章、第二章、第四章第二節及第六章第三節文字敘述似由原文直接翻譯，未加潤飾，使得文章敘述語句片斷呈現，無法組成完整語句，不易閱讀理解。

（七）本研究案希望透過國外電子商務風險管理措施（如電腦稽核、簽章認證等）及實施經驗，以及國內目前電子商務管理情形，瞭解電子商務的可行管理措施。報告中對於國內外風險管理措施相關資料豐富，但對國內外實施經驗及案例分析則較少著墨。

（八）封面、章節標記及版面配置，部分未依本會專案研究作業要點規定格式。

（九）報告中部分用詞請統一，如「提昇」或「提升」、「　謗」或「誹謗」、「違反」或「違犯」、「收集」或「搜集」等，錯漏字請再詳校更正。

研究小組修正紀錄之十

（一）本研究小組已將內容調整過，且於第八章內文，將短程、中程及長程具體建議事項，進一步加以詳細說明。

（二）於第八章已作詳細說明，其建構之規劃請參考圖 8-3 電子商務驗證組織架構圖。

（三）於第五章第三節中有提供相關有效管理電子商務的方法，各部門之分工請參考第八章之建議，在法令規章之建議上，即是有關電子商務評鑑機構的相關法令制定。

（四）政府機關對於資訊安全整體組織的調配，可參考圖 8- 1 電子商

務安全組織及風險管理服務中心人員架構圖，有關政府危機處理機制，有參閱第八章第四節之內容。

（五）此項建議已併入第七章第五節（五）結語的內文。

（六）已根據建議將第一章、第二章、第四章第二結及第六章第三節之文字敘述，加以潤飾，使得文章敘述語句較為通順，語句較完整。

（七）有關電子商務風險管理措施，可參閱第五章第三節之內文，有關國內外實施經驗及案例，可參考附錄（一）所提供相關網站。

（八）封面、章節標記及版面配置，已根據專案研究作業要點規定格式做適當的調整。

（九）報告中有部份用詞未統一用法已修正。

參考書目及網站

R1：電子商務總論

電子商務對於企業所能利用的範圍以及公司所經營的產業而言，已經佔有很大的企業潛在利益。而對於消費者來說，能得到的基本利益則是便利、資訊接取、及比價。而這些消費者的利益導致了更多的消費力量。本節將針對電子商務的基本架構作參考書輯的收集。

(一)王志平編著，”電子商務導論 Introduction of Electronic Commerence”，知 城數位科技股份有限公司，2001 年 9 月。

(二)黃京華編著，”電子商務總論”，五南圖書出版公司，2001 年 7 月。

(三)李進生、謝文良、林允永、蔣炤坪、陳達新、盧陽正著，”風險管理、風 險(VaR)理論與應用”，清蔚科技股份有限公司出版事業部，1987 年 9 月。

(四)簡井信行著、賴青松譯，”風險管理”，日之昇文化事業有限公司，1999 年 8 月。

(五)Efraim Turban, Jae Lee, David King, H. Michael Chung," ELECTRONIC COMMERCE –A MANAGERIAL PERSPECTIVE”, Prentice Hall, Upper Saddle River, NJ 07458，2000 年 11 月

(六)Marilyn Greenstein, Ph. D.，”Electronic Commerce：Security, Risk Management and Control”，Todd M Feinman，2000 年 9 月

R2：電子商務與網路安全

因為網際網路已經是一個合法全球性的公共設施。針對網路而言，一來必須增加彼此雙方連接的暢通性，二來也要同時增加彼此之間的安全防護。包含有公共的、私有的、即時的對策方法、持續改變的環境。而本節將針對電子商務與網路安全作參考書籍的收集。

(一) 賴溪松、葉育斌編著，”資訊安全入門”，全華科技圖書股份有限公司，2001 年 6 月。

(二) Seth T. Ross 著、馮志弘譯，”UNIX 系統保全工具”，美商麥格羅．希爾國際股份有限公司(台灣)，2001 年 3 月。

(三) David A. Bandel 著、安人玉、江安中、黃子綱、廖伸豐編譯，”LINUX 網路安全百寶箱”，旗標出版社，2001 年 3 月。

(四) Phillip G. Schein 著、白莫言譯，”Windows 2000 Security Design 認證教材—考前衝刺”，博碩文化出版有限公司，2001 年 9 月。

(五) 施威銘研究室著，”Norton Internet Security 網路安全大師 2001 玩家實例”，旗標出版社，2001 年 3 月。

(六) Simson Garfinkel with Gene spafford 著、李國熙、陳永旺譯，”電子商務與網路安全 Web Security & Commerce”，美商歐萊禮股份有限公司台灣分公司，2000 年 2 月。

(七) Ian McLean 著、安人玉、廖穎芝譯，”Windows 2000 網路安全深度探索”，旗標出版股份有限公司，2001 年 4 月。

(八) Efraim Turban, Jae Lee, David King, H. Michael Chung 著、張瑞芳等編著，”電子商務管理與技術”，華泰文化事業有限公司，2000 年 9 月。

(九) 郭再添、鄭玄宜著，”商業自動化與電子商務”，第三波資訊股份有限公司，2001 年 1 月。

(十) Robert S. Kaplan , David P. Norton，朱道凱譯，”平衡計分卡 THE

BALANCED SCORECARD 資訊時代的策略管理工具”, 城邦文化發行，2001 年 7 月。

(十一) 劉尚志、陳佳麟著，”網際網路與電子商務法律策略”，元照出版有限公司，2001 年 3 月。

(十二) 萬幼筠，“ 資訊安全管理 v.s.企業安全管理 ”，網路通訊，第 115 期，2001 年 2 月，（p24~p30）。

(十三) 施景彬、周嘉明，“ 企業 e 化的風險管理 ”，內部稽核，第 36 期，2001 年 7 月，（p14~p21）。

(十四) 林文隆，“ 網路銀行之風險管理與內部稽核 ”，內部稽核，第 36 期，2001 年 7 月，（p14~p21）（p25~p32）。

(十五) Ronald L. Krutz , Russell Dean Vines, ”The CISSP Prep Guide”, Wiley Computer Publishing, 2001 年 9 月。

(十六) Microsoft ,”Microsoft SNA Server4.0 Resource Guide”, 1999 年 9 月

(十七) Robert S. Macgregor , Alberto Aresi , Andreas Siegert , “WWW.Security “, IBM, 2001 年 11 月。

(十八) R. Bringle Bryant ,“UNIX CECURITY for the Organization” , SAMS publishimg, 2001 年 1 月。

(十九) Diane Stottlemyer, ”Automated Web Testing Toolkit”, Wiley Computer Publishing, 2001 年 5 月。

(二十) Bret Hartman, Donald J. Flinn, and Konstantin Beznosov, ”Enterprise Security with EJB and CORBA” Willey Computer Publishing, 2001 年 5 月。

(二十一) Peter Morath , ”secess@ e-bussiness”, THE McGRAW-HILL COMPANIES, 2000 年 9 月。

(二十二) Vijay Ahuja, Ph.D., ”Network & Internet SECURITY”, AP PROFESSIONAL, 1996 年 9 月。

(二十三) William Stallings, ”Network Security Essentials: Applications and Standards”, Prentice Hall, 2000 年 7 月。

(二十四) Mandy Andress, “Surviving Security：How to Integrate People , and Technology”, 2000 年 9 月。

R3：電子商務的行銷策略

本節將介紹幾本書。內容主要是針對電子商務現行發展的行銷策略，做為參考資料之用。

(一)比爾．本漢 (派傑公司)著、許梅芳譯，”電子商業產業版圖”，財訊出版社，2001 年 2 月。

(二)Martin V. Deise Conrad Nowikow Patrick King Amy Wright 著、陳正宇等合譯，”電子化企業經理人手冊”，ARC 遠擎管理顧問股份有限公司，2001 年 3 月。

(三)黃中杰編著，”企業經理人之經營 e 化入門書”，華彩軟體股份有限公司，2001 年 5 月。

(四)澤登秀明著、鍾雨靜譯，”行銷 e 時代行銷新趨勢”，博誌文化股份有限公司，2001 年 4 月。

(五)新谷文夫著、周慧君、曹晉穎譯，”突破 IT 經營的迷思 Information Technology 的經營法則與應用範例”，博誌文化股份有限公司，2001 年 3 月。

(六)大中華 EC 工作室編著，”大陸電子商務實戰手冊”，高寶有限股份公司，2000 年 11 月。

(七)Michael J. Mandel 著、曾郁惠譯，”網路大衰退”，聯經出版事業有限公司，2000 年 1 月。

(八)新谷文夫編著、許榮廷譯，”E Marketing 解讀顛覆世紀的 e 行銷案例”，博誌文化股份有限公司，2001 年 6 月。

R4：風險管理（risk management）與保險機制

【Reference And Web Sites】

(一) American Institute of Certified Public Accountant- Special Committee on Assurance Services." Assurance on risk Assessment." 1997. http://www.aicpa.org/assurance/scas/newsvs/risk/index.htm.

(二) Franckowiak, Dave." Risk Management and Internal Control." January 30, 1998. http://www.colybrand.com/industry/banking/ias/publications/risk_management.htm

(三) Frazier, David and Scott Spalding." The New SAS N0.78." CPA Journal,May 1996. http://www.luca.com/cpajournal/1996/0596/features/f40.htm.

(四) 風險管理學報 Journal of Risk Management：http://fhyu.mis.cycu.edu.tw/journal.htm

(五) 風險管理資訊系統發展之研究－以企業流程再造風險評估為例 A study of risk management information system development－Implementing with BPR risk evaluation：http://members.nbci.com/bus11/thesis/cover.htm

(六) 中華民國風險管理學會 Risk Management Society of Taiwan, 【R.O.C.】http://www.rmst.org.tw/

(七) Octa Soft 是一家企業對企業型網路金融系統、應用軟體與相關服務的供應商，其主要服務對象為全球各主要金融機構：http://www.octasoft.com/traditional_chinese/index.html

(八) IBM Software:E-commerce:Overview：**http://www-4.ibm.com/software/webservers/commerce/**

(九) IBM Software:E-commerce:WebSphere Commerce Suite,Start Edition:Overview：

http://www-4.ibm.com/software/webservers/commerce/wcs_start/

(十) IBM Software:WebSphere Commerce Suite Version 5.1：**http://www-4.ibm.com/software/webservers/commerce/netcomletter.html/**

(十一) IBM Software:E-commerce:ePIT：**http://www-4.ibm.com/software/webservers/commerce/epit/**

(十二) FreeMerchant.com：**http://www.freemerchant.com/press.htm**

(十三) Welcome to MerchantSystems.com-Express Commerce Gateway：**http://www.usmerchantsystems.com/products/i-pay.htm**

(十四) Visa-New Technologies-Internet Shopping Guide：**http://www.visa.com/nt/internet_shopping/safety/safety.jsp**

(十五) IBM Security：**http://www-3.ibm.com/security/library/wp_pc-chip.shtml**

(十六) IBM 4758 PCI Cryptographic Coprocessor：**http://www-3.ibm.com/security/cryptocards/index.shtml**

(十七) IBM PCI Cryptographic Coprocessor：**http://www-3.ibm.com/security/cryptocards/html/library.shtml**

(十八) IBM WebSphere: Solutions **http://www-4.ibm.com/cgi-bin/software.../b2csell.html&S_IACT=100AWWI0&S_CMP=campaig**

(十九) Hacker's Insurance:When All Else Fails：**http://www.sans.org/infosecFAQ/casestudies/insurance.htm**

(二十) ABCNEWS.com:Insurance Offered Against Hack Attacks：**http://www.abcnews.go.com/sections/tech/DailyNews/hackins**

urance000.10.html

(二十一) INSUREtrust.com LLC-Insurance/Services Center-e-Business Insurance Policies：
http://www.insuretrust.com/insurance.html

(二十二) TruSecure Corporation Security Solutions-Whitepapers：
http://www.trusecure.com/html/tspub/whitepaper_index.shtml

(二十三) Standard Publishing Corp：
http://www.standardpublishingcorp.com/ECOM-.html

(二十四) CFO-standard_publishing-Chapter 4:First-Party Risks：
http://home.aigonline.com/content/0,1109,4282-1047-cto,00.html

(二十五) CFO-standard_publishing-Chapter 5:Third-Party Risks：
http://home.aigonline.com/content/0,1109,4283-1047-cto,00.html

(二十六) Tivoli SecureWay Risk Manager Documentation：
http://www.tivoli.com/products/index/secureway_risk_mgr/sway_risk_mar_rel_docs.html

(二十七) Tivoli- Products- Tivoli SecureWay Risk Manager：
http://www.tivoli.com/products/index/secureway_risk_mgr/

(二十八) Tivoli- Manage.Anything. Anywhere：**http://www.tivoli.com/**

(二十九) Tivoli SecureWay News Clips from Around the World：
http://www.tivoli.com/products/solutions/security/secureway_news_clips_arch.html

(三十) SunGard_Infinity：
http://www.risk.sungard.com/infinity/index.html

(三十一) Also Suite: solutions elements：

http://www.algorithmics.com/solutions/sol_solcomponents.html

(三十二) Also Limits: Aligning firm-wire strategy with the daily activities of risk takers：
http://www.algorithmics.com/solutions/sol_algolimits.html

(三十三) Algorithmics: the benefits of an integrated risk management system：
http://www.algorithmics.com/solutions/benefits.html

(三十四) Algorithmics: enter Mark-to-Future：
http://www.algorithmics.com/solutions/enter-mtf.html

(三十五) ams- Global Risk Practice：
http://www.ams.com/GlobalRisk/
http://www.ams.com/GlobalRisk/feasibility.htm

(三十六) ams- AMS Europe：
http://www.ams.com/Europe/LCH5Year.htm

(三十七) ams- Global Risk Practice：
http://www.ams.com/GlobalRisk/LondonClearingHouseLtd.htm
http://www.ams.com/GlobalRisk/Opsynopsis.htm
http://www.ams.com/Eurpoe/riskmanager.htm
http://www.ams.com/GlobalRisk/RiskMgmtExDerivs.htm

(三十八) Internet Solutions Practice：
http://ams.com/ItJustMakesSense/MaturityModels.htm

(三十九) Library：**http://www.certco.com/library.shtml**

(四十) SME e-toolkit：
http://www.ifc.org/sme/html/sme_e-toolkit.html

(四十一) INSUREtrust.com LLC-Total LifeCycle Solutions：
http://www.insuretrust.com/lifecycle.html

(四十二) INSUREtrust.com LLC-Total LifeCycle Solutions- e-Business Risk Management Services：
http://www.insuretrust.com/services.html

(四十三) INSUREtrust.com LLC-Total LifeCycle Solutions- e-Business Insurance Policies：
http://www.insuretrust.com/insurance.html

(四十四) INSUREtrust.com LLC-Total LifeCycle Solutions- e-Business Risk Management -Why is it Important?：
http://www.insuretrust.com/ebizatrisk.html

(四十五) Hiscox-template policy page：
http://www.hiscox.com/p_i/cyber_summary.stm

(四十六) Fraud Management：
http://www.hnc.com/business_03/fs_03/fraudmgmt_030107?

(四十七) Financial services：**http://www.efalcon.com/**

(四十八) MIS Products：**http://www.misti.com/Products.asp**

(四十九) FM Global Introduces eConomy：
http://www.fmglobal.com/news/releases/20010416.html

http://www.fmglobal.com/library/speeches/cyberspace.html

(五十) Deloitte & Touche: Enterprise Risk Services：
http://www.dttus.com/Risk/customers/services/webtrust/

(五十一) Amenaza Technologies Limited：http://www.amenaza.com/

(五十二) SecurITree | Methodology：
http://www.amenaza.com/securitree2.html

(五十三) Consulting Services | Amenaza Way：
http://www.amenaza.com/consulting2.html

(五十四) 一般公司：

http://www.scmagazine.com

http://www.tivoli.com/products/solutions/security/

http://www.ibm.com/services/e-business/security.html

http://www.microsoft.com/security/

http://www.wwwhack.com

http://www.securityprotal.com/

http://www.cs.princeton.edu/sip/

http://www.cve.mitre.org/

http://infosyssec.com/

http://cses.ed.gov/pubsearch/pubsinfo.asp?pubid=98297

http://www.geocities.com/SiliconValley/Bay/9952/

http://www.viacorp.com/crypto.html

(五十五) 駭客：

http://www.hackernews.com/

http://hacktivism.tao.ca/