楊欣哲、林裕倫（2014），『企業資訊網站設計之資訊安全的評估模式與評量工具之研究』，*資訊管理學報*，第二十一卷，第二期，頁 107-138。

企業資訊網站設計之資訊安全的評估模式與評量工具之研究

楊欣哲*
東吳大學資訊管理學系

林裕倫
東吳大學資訊管理學系

摘要

由於全球資訊網（World Wide Web）技術發展與應用普及，因此帶動了企業資訊網站平台的興起。然而，提供安全的企業資訊網站平台（EIP）是網際網路應用之重要的服務品質關鍵之一。

有鑑於此，本論文主要在針對企業資訊網站平台設計上之各種不同的風險構面，參照 ISO27001 文獻和國際標準組織 OWASP 與 SANS 組織所提出的資訊網站之風險，透過 ISMS 模式找出每一風險構面與風險因子以及經由專家焦點座談確認，並經由 5 位資訊安全或 Web 網站系統建置之專家或學者填寫各項構面因子問卷，再利用 AHP 層級分析法，計算出各項風險權重值與排序。然後，將制訂 EIP 之資訊安全的評估模式與評量工具。最後，我們將以現有的企業網站資訊平台，採用本論文所提出的資訊安全評估模式與評量工具來計算企業資訊網站平台之風險值，並且依風險值訂定風險等級的指標以驗證資訊網站之安全性，並提出相關改善策略之建議。總之，我們所提出的資訊安全之評估模式與評量工具，可用來作為安全的網頁系統建置之安全評量準則與參考模式。

關鍵詞：企業資訊網站、評估模式、AHP、資訊安全、評量工具

* 本文通訊作者。電子郵件信箱：sjyang@csim.scu.edu.tw
2013/05/3 投稿；2014/03/02 修訂；2014/03/31 接受

Yang, S. J. and Lin, Y. L. (2014), 'An Approach to Assessment Model and Metric Tool of Information Security in Designing EIP', *Journal of Information Management*, Vol. 21, No. 2, pp. 107-138

An Approach to Assessment Model and Metric Tool of Information Security in Designing EIP

Shin-Jer Yang*
Department of Computer Science and Information Management, Soochow University

Yu-Lung Lin
Department of Computer Science and Information Management, Soochow University

Abstract

The WWW technology brings the rising of Enterprise Information Portal (EIP). However, providing a secure Enterprise Information Portal is one of essential quality of services (QoS) in Internet applications.

Based on the security of designing EIP, the purposes of this paper are to find out various risk facets based on ISO 27001 reference standards and the ISMS process and also utilize AHP model to validate the factors of each risk facet using focus discussion of experts. Then, we refine and validate required factors of each risk facet through questionnaire method of five experts or scholars who are specialized in implementing a secure EIP system. In addition, we can establish an Information Security assessment model of EIP and design its algorithm. Finally, we develop a Metric Tool and also perform experiments to verify and validate the risk management of a selected EIP practice. According to the risk values, it can refine the risk level to verify and validate the security of EIP and propose related improving strategies. Based on the experimental result, our proposed assessment model and Metric Tool of EIP Information Security can be served as the security measure guidelines of implementing a secure Web application.

Keywords: EIP, Assessment Model, AHP, Information Security, Metric Tool

* Corresponding author. Email: sjyang@csim.scu.edu.tw
2013/05/03 received; 2014/03/02 revised; 2014/03/31 accepted

壹、緒論

一、研究背景與動機

由於全球資訊網（WWW）與網際網路（Internet）的應用與技術成熟，使得企業使用資訊網站平台也越來越廣泛，例如：銀行業、保險業、零售商業、房仲業、電子科技業…等企業，皆利用資訊網站平台來增加其商業價值。

資訊網站平台設計架構皆可分為前台與後台之架構，這兩部份所產生的安全性問題也非常多。隨著網路應用程式的發展，許多層出不窮的攻擊事件始終影響網路服務的使用。近幾年來，民間企業及政府機關資訊網站的安全危機，大部分都是來自於駭客利用資訊網站本身存在的弱點所進行的攻擊。

在資訊網站平台廣泛運用下，網路安全漏洞的大量存在和不斷發現新問題，仍是網路安全的最大隱憂。我們該如何有效防範資訊網站的安全性，以防資料外洩與資料損毀。而企業資訊網站平台設計之安全性所產生的問題，通常是經由 Server 端與 Client 端所引起的。因此，該如何有效地防範攻擊事件的問題，安全性問題變成企業資訊網站設計的焦點之一。

二、研究目的與範圍

由於本研究範圍所針對的企業資訊網站是在不同作業系統、動態網頁技術及資料庫管系統所建置，因此將範圍歸類分為 Server 與 Client 端，並找出相關的風險因子，分析每個因子的風險值，利用 AHP 層級分析法（Analytic Hierarchy Process），為企業資訊網站訂定其風險等級，最後提出企業資訊網站平台之資訊安全改善策略之建議。有鑑於此，本論文主要的研究目的如下：

1. 參考相關資訊安全的文獻，並針對企業資訊網站平台找出其風險構面，然而，再針對每個風險構面所產生的風險因子逐一分析。
2. 使用資訊安全評估模式分析企業資訊網站平台的安全性，並且提出網站風險值及風險層級。
3. 然後，將依照此評估模式設計一套評量工具，再以實例來進行實證，以驗證本文所提出的企業資訊網站之資訊安全的評估模式。
4. 此外，將對於各個不同層級的風險值之企業資訊網站平台，所產生出的安全問題，提出相關可能改善策略之建議。

三、研究流程與說明

本論文的研究步驟可分為六個步驟進行。首先為相關文獻收集與研讀，蒐集與研究 ISO27001 標準之服務品質需求與資訊管理安全系統運作模式；第二步驟將整理文獻與 OWASP 組織所提出來的 Web 網站風險，並經由第一階段專家問卷確認風險構面與因子，之後利用第二階段 AHP 專家問卷分析計算出各項構面與因子之權重值；第三步驟將根據資訊安全準則，設計一套企業資訊網站之資訊安全評估模式與演算法；第四步驟將設計一套資訊安全之評量工具，並選擇一企業資訊網站平台作為實證；第五步驟為分析實證結果，並依照其風險因子提出相關改善策略之建議；最後為改善後結果分析與完成論文撰寫。

四、論文章節架構說明

第壹章是緒論；包括研究背景與動機和研究目的與範圍；第貳章是文獻探討與相關研究；探討企業資訊網站安全之應用，並且對於其資訊網站產生的資訊安全構面作評估，及分析各種資訊安全構面所產生的因子與現有的文獻及相關研究作一概述；第參章是專家問卷分析；本論文利用兩階段的專家問卷對資訊安全構面與資訊安全因子進行分析，並計算出資訊安全因子權重值與其排序。第肆章是資訊網站之資訊安全的評估模式與系統設計方法；首先，會參照 ISO 27001 標準以及 ISMS 流程，然後透過專家之焦點座談以及經 5 位資訊安全或 Web 網站系統建置之專家或學者問卷調查予以確認各項構面因子，並利用 AHP 層級分析法計算出權重值，以及針對企業資訊網站之資訊安全，提出一資訊網站安全之評估模式。然後，根據此資訊網站評估模式訂定出網站資訊安全等級；第伍章是評量工具與改善策略；採用本論文所提出的企業資訊網站之資訊安全評估模式為設計準則，設計一套資訊網站之資訊安全的評量工具，並且利用某企業現有的資訊網站平台做為實證與分析結果，並提出相關改善策略建議。第陸章是結論：說明本論文之研究成果與貢獻以及未來的研究建議。

貳、文獻探討及相關研究

本章將回顧過去的研究文獻，並將文獻探討分為四個部分：企業資訊網站之應用與風險構面評估、ISO 27001 標準和資訊安全管理系統（Information Security Management System，ISMS）運作模式介紹、各種風險構面之因子分析以及 AHP 層級分析法的介紹。

一、企業資訊網站之應用與風險構面評估

隨著 E 化時代的來臨，使用電子商務網站已變成企業重要的獲利工具之一，不過在此蓬勃發展之下，相對的許多網站風險因素也相依產生。每個網站或多或少都會有風險因素存在，然而這可能會造成服務品質上的一些缺失。因此，評估網站風險構面，以預防降低服務上所發生的錯誤，是有其必要性的。

企業資訊網站之風險涵蓋的層面，包括了 Web 應用層、資料庫、作業系統、人為管理、網路應用等（Cachia & Micallef 2007）。而這些層面所涵蓋的風險可能存在許多風險因子，正是企業資訊網站所面臨的最大難題，許多層出不窮的系統安全弱點和漏洞仍然存在於企業資訊網站環境中。事實上，資訊安全是企業於資訊網站上之電子商務和 e-化企業應用上特別重視的議題之一（Yang & Wan 2008）。因此，本章第三節將會對各種風險構面之風險因子作一詳細的分析。

二、ISO 27001 標準與資訊安全管理系統運作模式

ISO 27001 是透過風險評估、風險管理、資訊安全組織、資產管理、人力資源安全、實體與環境安全、存取控制、系統開發及維護、營運持續管理及通訊與作業管理等（ISO 27001 2005），從這些標準引導企業對於資訊安全進行控制和管理，以有效降低企業組織所面臨的資訊安全風險。ISO 27001 標準可作為整個企業之資訊安全管理系統評估的基準，而目的在於定義及提供企業做為保護自身或客戶之關鍵資訊。所以，作好企業資訊網站安全首要的就是找出風險構面所存在的風險因子，進而才能達到網站的機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）等資訊網站安全特性：

1. 確保資訊的機密性（Confidentiality）：
   - 確保只有獲得授權的人才能存取資訊。
   - 保護資訊不被非法存取或揭露。
2. 確保資訊的完整性（Integrity）：
   - 確保資訊與處理方法的精確性與完整性。
   - 確保資訊沒有不當的修改或損毀。
3. 確保資訊的可用性（Availability）：
   - 只有經過授權的用戶在需要時可以存取資訊並使用相關資訊資產。
   - 資料必需即時並可靠的提供給企業內部各個層級的使用需求。

在運用 ISO 27001 過程方法中，資訊安全管理系統所突出的重要性如下（Barafort et al. 2006）：

1. 了解公司的資訊安全要求以及需要的資訊安全政策和目標。
2. 執行和操作控制管理公司的資訊安全風險的範圍內相應的整體經營風險。

3. 監測、有效的審查和 ISMS 的績效。

4. 持續的改進以客觀測量為基礎。

而這些都是國際標準採用的模型構建用來建置 ISMS 的所有過程（Allen 2000），其使用 ISO 27001 作為建構的準則（ISO 27001 2005; ISO/IEC 27005 2008），依據此準則建立 ISMS、識別各項風險之後建立風險處理計畫（韓慧林等 2011），搭配定期稽核來維持與改進 ISMS，以確保組織的資訊安全。藉由適當的手段與方法予以降低或轉移，而是讓企業組織選擇所能容忍的風險水準，並排除無法承擔的風險，因此 ISMS 是建立在風險評鑑與管理的基礎上。

三、各種風險構面之風險因子分析

實際上，網站上的安全性弱點（vulnerability）是一種程式設計上的不良或者疏忽，再運作過程中可能產生一些問題（SANS TOP 20; Allen et al. 2000），導致程式運作的結果不是我們所預期的狀況，讓攻擊者藉機對使用系統做出不當的行為，例如：資料洩漏、控制作業系統、或不法獲得未經授權的許可…等。大部分的弱點是來自於應用程式或者作業系統設計上的缺陷，另外人為的管理疏失，也可能帶來相當大的風險，造成企業資訊網站運作上之資訊安全的危機。

本論文根據 OWASP（Open Web Application Security Project）於 2011 年提出的 OWASP Top 10 網站安全風險的安全性問題（Category: OWASP Top Ten Project），可反映出目前網路應用攻擊型態的變化，如表 1 所示。

表 1：2011 年 OWASP Top 10 網站安全風險

名次	風險因子名稱
1	注入弱點（Injection）
2	跨站腳本攻擊（Cross Site Scripting）
3	身分驗證功能缺失（Broken Authentication and Session Management）
4	不安全的物件參考（Insecure Direct Object Reference）
5	跨站冒名請求（Cross Site Request Forgery）
6	網站安全組態不當設定（Security Misconfiguration）
7	未加密的儲存設備（Insecure Cryptographic Storage）
8	無權限的控制（Failure to Restrict URL Access）
9	不安全的網路傳輸（Insufficient Transport Layer Protection ）
10	未驗證的網路重新導向（Unvalidated Redirects and Forwards）

另外，本論文依據 SANS TOP 20，可將資訊網站安全之風險類型依兩大類型來區分，分別為伺服器端與客戶端類型（林玉峰 2005; Fenz 等 2007），其中伺服器包含了 Web 應用、作業系統、以及資料庫，然而作業系統與資料庫主要是應用軟體本身設定相關參數安全作評估；客戶端則以網路應用為最常見。以下是初步整理的各項構面所之風險所會引起的風險因子，如表 2 所示。

表 2：企業資訊網站平台之風險因子

類型	風險構面	風險因子	相關文獻參考來源
伺服器端	網頁應用構面	注入弱點	OWASP Top 10 與 SANS Top 20
		跨站腳本攻擊	
		身分驗證功能缺失	
		不安全的物件參考	
		跨站冒名請求	
		網站安全組態不當設定	
		未加密的儲存設備	
		無權限的控制	
		不安全的網路傳輸	
		未驗證的網路重新導向	
	資料庫構面	SQL Server	Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard 與本研究整理
		Oracle	
		My SQL	
		DB2	
		Informix	
		Sybase	
	作業系統構面	Microsoft Windows	Allen 等（2000）與本研究整理
		Linux	
		UNIX	
	網路應用構面	資料外洩	A Multi-Tier, Multi-Role Security Framework for E-Commerce Systems 與本研究整理
		SOP 流程疏失	
		管理人員資訊技術不足	
		人為操作不當	
		資料誤用	
		資料鍵入錯誤	

類型	風險構面	風險因子	相關文獻參考來源
客戶端	人為管理構面	Web browsers	An Approach to Separating Security Concerns in E-Commerce Systems at the Architecture Level 與本研究整理
		E-mail	
		Media Players	
		FTP	
		Telnet	
		Backup Software	
		Anti-virus Software	
		Office Software	

四、層級分析法（AHP）

本節接下來將對 AHP 作詳細逐一介紹，以及 AHP 所使用的步驟和本論文所使用的 AHP 應用軟體。

（一）AHP 介紹

本研究以層級分析法（Analytic Hierarchy Process，以下簡稱 AHP），為美國匹茲堡大學教授 Thomas L. Saaty 於 1971 年所提出的決策分析工具，主要應用在不確定情況下極具有多數個評估準則的決策問題上（翁宇能 2009; Saaty 1990; Saaty 1980）。對於決策者而言，階層結構有助於對於事物的了解，但在面臨「選擇是當方案」時，必須根據某些基準進行各替代方案的評估，以決定各替代方案的優勢順序（priority），從而找出適當的方案。

層級分析法經由層級分解方式，將複雜的問題系統化，經由量化的評分判斷逐層分析各項要素的權重，做為整體參考的依據。

（二）實施步驟

本文在 AHP 方法在使用上，分為兩部分，一個是建立層級，另一個是層級的評估，AHP 法是將複雜的問題，交由專家學者評估出要素之後，再以簡單層級結構表示，接著再以尺度評估來做成要素的成對比較且建立矩陣，然後求得特徵向量，再比較出層級要素的先後順序；之後在檢驗成對比較矩陣的一致性，看看有無錯誤，是否可以作為參考（翁宇能 2009; 羅福枝 2005; 鄧振源&曾國雄 1989），各相關步驟說明如下。

1. 問題的界定：對於問題所可能涵蓋的範圍，應盡量的擴大，使影響問題的因素，均可納入問題中。本研究的問題界定在企業資訊網站之資訊安全的評估。
2. 建構層級結構：首先，需先列出和決策目標有關之決策因素，並依相互關

係建構為層級架構。本研究透過文獻探討與專家訪談的方式建構此層級

3. 建立成對比較矩陣：某一層級的要素，以上一層級某一要素做為評估基準下，進行要素間的成對比較。若有 *n* 個要素時，則需進行 *n*（*n*-1）/2 個成對比較。
4. 問卷設計與調查：本研究經相關文獻探討及專家學者意見，規劃出本研究的問卷架構。AHP 是以成對比較的方式進行，所以問卷的設計是以成偶比較做為評估方式，如表 3。由相對強弱程度的不同給予分數，而評估尺度意義及說明，如表 4 所示（施藍欣 2008）。
5. 計算特徵值與特徵向量：成對比較矩陣得到後，即可求取各層級要素的權重。使用數值分析中常用的特徵值解法，找出特徵向量或稱優勢向量。
6. 層級一致性檢定：求取各層級一致性指標（Consistency Index，C.I.）如公式(1)與一致性比率（Consistency Ratio，C.R.），檢定成對比較矩陣的一致性。

$$C.I.=\frac{\lambda\max-n}{n-1} \tag{1}$$

表3：成偶比較評估表

尺度	非常重要 9	8	相當重要 7	6	重要 5	4	稍為重要 3	2	同等重要 1	2	稍為重要 3	4	重要 5	6	相當重要 7	8	非常重要 9	尺度
要素																		要素
A																		B
A																		C
A																		D
B																		C
B																		D
C																		D

表 4：AHP 評估尺度意義及說明

評比尺度	定義	說明
1	同等重要	兩方案具同等重要性
3	稍微重要	經驗與判斷顯示稍微偏向某一方案
5	重要	經驗與判斷強烈喜偏向一方案
7	相當重要	實際顯示非常強烈偏向某一方案

9	非常重要	有足夠證據證明偏向哪一方案
2，4，6，8	中間值	折衷值

資料來源：Saaty 1980

當一致性指標 C.I.≦0.1 時，則可獲得較滿意的一致性（Saaty 1980）。從評估尺度所產生的正倒值矩陣，在不同階數下，產生不同的 C.I.值，稱為隨機指標（Random Index，R.I.），其值隨矩陣階數之增加而增加，而 R.I 使用時通常不自己去計算，而是使用 Saaty 所歸納出來的隨機指標表，如表 5 可得知。

表 5：隨機指標數值表

階數	1	2	3	4	5	6	7	8
R.I.	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41
階數	9	10	11	12	13	14	15	
R.I.	1.45	1.49	1.51	1.48	1.56	1.57	1.58	

在相同階層數的矩陣下，C.I.值與 R.I.值的比率，稱為一致性比率（Consistency Ratio，C.R.）即公式(2)所示。

$$C.R. = \frac{C.I.}{R.I.} \tag{2}$$

（三）AHP 應用軟體

由於 AHP 之理論被廣泛的運用在各種不同研究上，而各種電腦輔助計算程式也大多成熟，故本研究採用「Expert Choice 11.5」軟體來進行回收後問卷分析之應用軟體。在資料輸入成對矩陣後，軟體自動計算出 C.R.值與相對權重值。

參、專家問卷分析

本研究將 AHP 的評估因子分為二階段調查進行，在第一階段的專家焦點座談中將從文獻找出的風險指標進行重要性評估，由具網站建置實務經驗的資訊安全專家初步評選適合的指標供第二階段之專家或學者問卷調查並作分析使用。

一、第一階段：焦點座談

本研究第一階段焦點座談將以 Likert （1932）之五點評量尺度之方式將各指標之重要性分為「非常不重要」、「不重要」、「無意見」、「重要」、「非常

重要」5 等分，依序將重要性由低至高區分為 1~5 分，根據專家對各項指標的重要性評估給分，初步的評估適合評估的風險因子指標。

由於本文所提出的評估風險因子指標是參照文獻與國際標準組織所提出的網站風險因子，於第一階段中透過三位專家如附錄一之焦點座談方式，共同訂出相關風險因子，其主要的目的是找出專家所重視的指標，以此作為評估時參考的依據，並用於第二階段問卷調查時進行 AHP 層級分析。因此，本研究選取在第一階段調查中之重要性評估為得分為 3 分以上等級者做為進一步研究之評估指標項目。從表 6 中第一階段調查結果可看出，只有 Web 應用構面的無權限控制風險因子指標低於標準值 3，所以並未納入第二階段 AHP 問卷指標項目。

表 6：第一階段焦點座談調查結果

評估構面	評估因子	平均	標準	符合
網頁應用構面	注入弱點	4.67	3	Y
	跨站腳本攻擊	4.33	3	Y
	身分驗證功能缺失	4	3	Y
	不安全的物件參考	4.33	3	Y
	跨站冒名請求	4	3	Y
	網站安全組態不當設定	3.67	3	Y
	未加密的儲存設備	3.33	3	Y
	無權限的控制	2	3	N
	不安全的網路傳輸	3.33	3	Y
	未驗證的網路重新導向	3	3	Y
資料庫構面	SQL Server	4.67	3	Y
	Oracle	3.67	3	Y
	My SQL	4.33	3	Y
	DB2	3	3	Y
	Informix	3	3	Y
	Sybase	3.33	3	Y
作業系統構面	Microsoft Windows	4.67	3	Y
	Linux	3.33	3	Y
	UNIX	3	3	Y
網路應用構面	Web browsers	4.67	3	Y
	E-mail	4.33	3	Y

	Media Players	3.67	3	Y
	FTP	3.33	3	Y
	Telnet	3.33	3	Y
	Backup Software	3.33	3	Y
	Anti-virus Software	3.67	3	Y
	Office Software	3	3	Y
人為管理構面	資料外洩	4.67	3	Y
	SOP 流程疏失	4	3	Y
	管理人員資訊技術不足	4	3	Y
	人為操作不當	3.33	3	Y
	資料誤用	3.67	3	Y
	資料鍵入錯誤	3	3	Y

二、第二階段：問卷實施與分析

本節將進行專家或學者問卷調查並使用 AHP 方法加以分析，以及介紹專家或學者之背景資料、說明問卷回收統計和問卷結果分析。

（一）專家背景介紹

本論文之專家問卷所實施對象是在於 Web 網頁建置有相關經驗或是資訊安全、網路安全方面、系統安全、資料庫安全等，有相關專長或工作經驗之資深專家或學者，其詳細背景如附錄二。

（二）專家問卷回收統計

經由電話與 e-mail 邀約專家訪談，共 6 專家回應願意接受訪談，訪談時間為 2012 年 2 月 10 日到 3 月 20 日，最後於 3 月 31 日完成問卷回收，總計回收 6 份問卷，其中 1 份一致性比率 C.R.值大於 0.1，不符合 AHP 理論的基本要求，故視為無效問卷，不加入整體問卷的分析討論，有效問卷共 5 份，專家問卷回收統計表如表 7 所示（未列入無效問卷之專家）。

表 7：AHP 專家問卷回收統計表

	分數	百分比
發出問卷	6	100
回收問卷	6	100
無效問卷	1	17

	分數	百分比
有效樣本	5	83

（三）專家問卷結果分析

經由第二階段專家問卷整理後，採用 AHP 分析軟體以分析出各項構面與風險因子之權重值。由各項構面與風險因子之架構圖，可得知在企業資訊網站之資訊安全各項構面相對權重，以網頁應用構面（0.382）相對權重最高，作業系統構面（0.220）為次之，第三為網路應用構面（0.181），第四為人為管理構面（0.118），資料庫構面（0.099）為最後，構面整體 C.R. = 0.00342 < 0.1 通過一致性的比率檢定，其詳細分析圖如圖 1，而依照權重值大小排序表，如表 8 所示。

圖 1：各項構面之相對權重圖

表 8：各項構面之相對權重表

風險因子	權重值	排序
Web 應用構面	0.382	1
作業系統構面	0.220	2
網路應用構面	0.181	3
人為管理構面	0.118	4
資料庫構面	0.099	5

以下將依序分別為各項構面的風險因子相對權重值之分析表逐一作詳細說明。Web 應用構面之風險因子權重值排序從大到小為：跨腳本攻擊（0.228）、注入弱點（0.198）、不安全的物件參考（0.121）、身分驗證功能缺失（0.101）、未驗證的網路重新導向（0.100）、不安全的網路傳輸（0.085）、跨站冒名請求（0.073）、網站安全組態不當設定（0.051）、未加密的儲存設備（0.044），其詳細資料如表 9。

資料庫構面之相對權重值分析表可得知排序大到小為 SQL Server(0.292)、My SQL（0.248）、Oracle（0.216）、DB2（0.132）、Informix（0.06）、Sybase（0.053），詳細資料表如表 10。從表 11 看出，作業系統構面之相對權重值分析表可看出，Microsoft Windows（0.461）為第一，次之是 Linux（0.347），而 UNIX（0.193）為最後。另外，從表 12 可看出網路應用構面之相對權重值分析表可得知排序大到小為：Web browsers （0.268）、E-mail （0.226）、FTP （0.146）、Telnet （0.128）、Media Players （0.080）、Anti-virus Software （0.069）、Backup Software（0.043）、Office Software（0.039）。最後，人為管理構面之相對權重分析表如表 13 所示，資料外洩（0.350）、人為操作不當（0.212）、SOP 流程疏失（0.143）、管理人員資訊技術不足（0.115）、資料誤用（0.095）、資料鍵入錯誤（0.085）。

表 9：Web 應用構面之相對權重分析表

風險因子	權重值	排序
跨站腳本攻擊	0.228	1
注入弱點	0.198	2
不安全的物件參考	0.121	3
身分驗證功能缺失	0.101	4
未驗證的網路重新導向	0.100	5
不安全的網路傳輸	0.085	6
跨站冒名請求	0.073	7
網站安全組態不當設定	0.051	8
未加密的儲存設備	0.044	9

表 10：資料庫構面之相對權重分析表

風險因子	權重值	排序
SQL Server	0.292	1
My SQL	0.248	2
Oracle	0.216	3
DB2	0.132	4
Informix	0.06	5
Sybase	0.053	6

表 11：作業系統構面之相對權重分析表

風險因子	權重值	排序
Microsoft Windows	0.461	1
Linux	0.347	2
UNIX	0.239	3

表 12：網路應用構面之相對權重分析表

風險因子	權重值	排序
Web browsers	0.268	1
E-mail	0.226	2
FTP	0.146	3
Telnet	0.128	4
Media Players	0.080	5
Anti-virus Software	0.069	6
Backup Software	0.043	7
Office Software	0.039	8

表 13：人為管理構面之相對權重分析表

風險因子	權重值	排序
資料外洩	0.350	1
人為操作不當	0.212	2
SOP 流程疏失	0.143	3
管理人員資訊技術不足	0.115	4
資料誤用	0.095	5
資料鍵入錯誤	0.085	6

經由 AHP 專家問卷分析軟體可計算出每位專家之問卷結果，有五位專家之問卷的一致性檢定 C.I 皆小於 0.1，表示決策者在建立成對比較矩陣時，此成對比較矩陣的一致度視為滿意。而在每一階層的一致性比率 C.R.也皆小於 0.1，表示決策者在建立成對比較矩陣時，對於各要素權重判斷的偏差程度尚在可接受的範圍內亦即具有一致性，風險構面之一致性檢測結果如表 14 所示。

表 14：風險構面之一致性檢測

風險構面	C.I.	R.I.	C.R	通過一致性（C.R≦0.1）
Web 應用構面	0.00458	1.45	0.00316	Y
資料庫構面	0.00248	1.24	0.002	Y
作業系統構面	0.00150	0.58	0.0026	Y
網路應用構面	0.00898	1.41	0.00637	Y
人為管理構面	0.00339	1.24	0.00273	Y

肆、資訊網站之資訊安全評估模式與演算法設計

本章我們將針對企業資訊網站平台，建置一資訊安全之處理架構，並且根據此架構衍生出一個具企業資訊網站之資訊安全的評估模式，以及發展此方法的演算法，並以此架構作為建置安全性的企業資訊網站平台之基準。

一、資訊安全評估模式制定

彙總相關文獻資料及對企業資訊網站平台現況進行調查，找出企業資訊網站之資訊安全的評估模式，運用 AHP 層級分析法找出企業資訊網站平台之資訊安全的重要因素及優先順序 （陳俊德 2009）。本文之研究架構如圖 2 所示，其架構詳細說明如下：

1. 先瞭解企業資訊網站平台安全的需求（蒐集相關文獻）
2. 影響企業資訊網站平台安全之風險因子（專家訪談）
3. 提出企業資訊網站資訊安全管理層級架構
4. 建立企業資訊網站之資訊安全評估項目的權重值（利用 AHP 方法）
5. 制定企業資訊網站之資訊安全的等級

依照企業資訊網站平台的資訊安全需求考量，本研究參照 ISO 27001 制定了資訊安全之評估模式，以確保網路服務正常、網站系統持續運作、防止病毒、駭客等入侵及破壞行為、防止他人不當使用。然而，此企業資訊網站之資訊安全評估範圍適用於 Client 端與 Server 端。本研究將計算出企業資訊網站系統之資訊安全因子的資訊安全值，為了保持客觀與鑑別度，因此本論文改良 ISO 27001 所提出的四個風險等級，將企業資訊網站之資訊安全等級分為五種等級，依序分別為 A、B、C、D、E 五種資訊安全等級，可接受等級為 D、E 如表 15 所示。

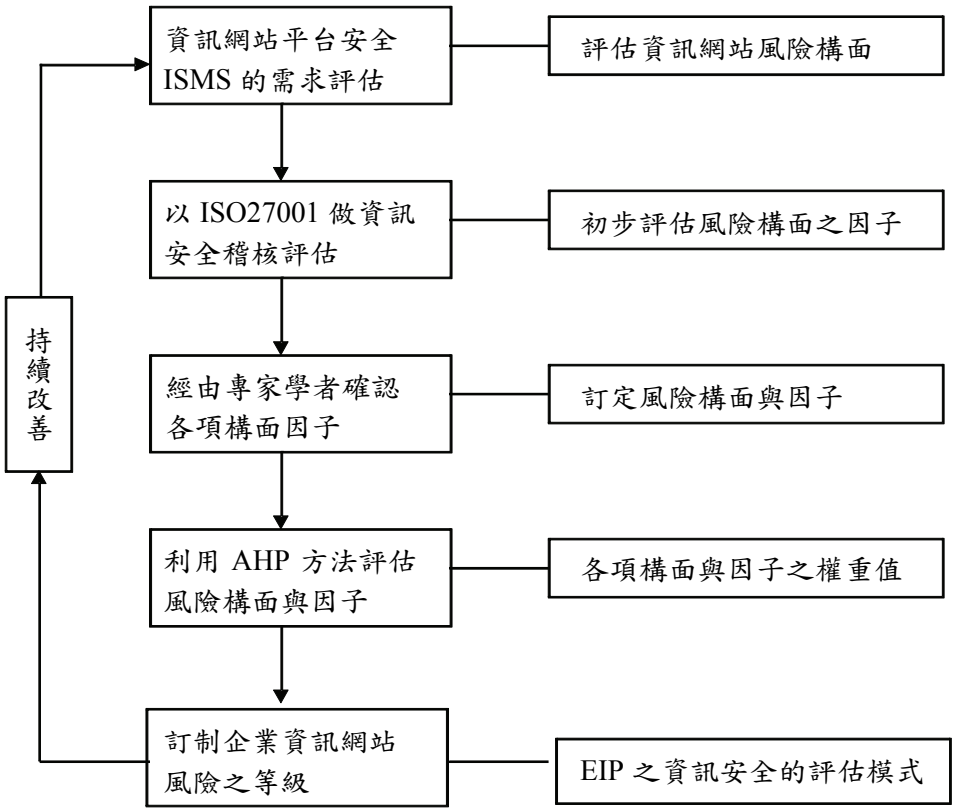

圖 2：研究方法架構

表 15：風險層級

等級	初始值	結束值	說明
A	400	500	立即改善
B	300	399	需要改善
C	200	299	需要注意
D	100	199	勉強接受
E	0	99	可以接受

二、資訊安全之評量工具設計原理與演算法

本論文將依照此企業資訊網站平台之資訊安全的評估模式如圖 3 所示，而提出其評估方法。本節將設計此方法的步驟及演算法，其演算法之虛擬碼如下：

```
Main EIP_WEB-RISK( )
{ int Total_Risk;
For (int n =1;; n++){
  int Facet_val , Factor _val;
  Facet_val    = Procedure Select_Facet();
  Factor _val = Procedure Select_Factor();
  Total_Risk    +=    Procedure Evaluation_Risk (Facet_val, Factor _val);
If (n > 10) break;    // The tools restrictions;
}
Print Total_Risk;    // The sum of risk value
}
Procedure Select_Facet()
{ int i = Facet. getSelectedValue ();// Select the Facet data;
      int Facet_value = AHP(i); //Through AHP calculated risk Facet value;
      return    Facet _value;
}
Procedure Select_Factor()
{ int x = Factor. getSelectedValue(); // Select the Factor data;
      int Factor _value = AHP(x); //Through AHP calculated risk Factor value;
      return    Factor _value;
}
Procedure Insert_Data()
{    int val = text.getInsertValue(); // Input the info of protected value;
      Error_Check(val);
      return val;
}
Procedure Error_Check(val)
{
      If length of value is over limit then
      print error message;
      End if
      If data type is incorrect then
      print error message;
      End if
```

```
        If field is null then
        print error message;
        End if
        check that the content of value is valid;
    }
    Procedure Evaluation_Risk(Facet_val, Factor _val)
    {
    int Security_value,risk_value,protect_value;
    risk_value = Facet_val * Factor _val;
    protect_value = Insert_Data();
    Security_value = risk_value * protect_value; // Calculate the Security value;
    return Security_value;
     }
    END EIP_WEB-RISK.
```

此演算法的主程式為 EIP_WEB-RISK，內容包括本論文所具企業資訊網站平台之資訊安全評估之應用程式架構，其中又包含了五個程序 Select_Facet、Select_Factor、Insert_Data、Error_Check、Evaluation_Risk，其功能分別為：

1. Select_ Facet （）：使用者選擇所要評估的風險構面。
2. Select_Factor（）：使用者選擇所要評估的風險因子。
3. Insert_Data（）：使用者選擇輸入風險因子之防護程度。
4. Error_Check（）：錯誤檢測，過濾使用者的輸入資料，避免錯誤產生。
5. Evaluation_Risk（）：評估資訊網站之資訊安全，並顯示其風險值與風險排序。

此外，本演算法的主要目標是在設計一套企業資訊網站平台之安全性評量工具。根據專家建議訂出所需評估的風險構面與各項風險因子，利用 AHP 專家問卷分析軟體計算出風險構面與風險因子之權重值，並依照風險因子之排序大小，來訂定此評量工具之計算方式。然後，我們請使用者輸入該企業資訊網站之資訊安全相關評估的資料。最後，利用此評量工具對企業資訊網站之資訊安全作安全性評估，計算出該網站風險值，並依照不同風險值給予不同風險等級。

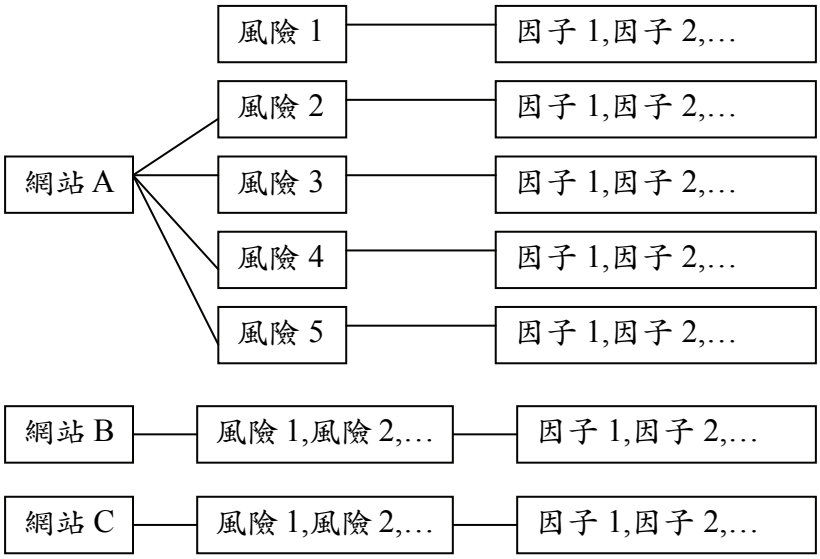

圖 3：企業資訊網站之資訊安全評估方法

伍、評量工具與改善策略

本章將分為四個小節進行，首先會先介紹本論文所設計的企業資訊網站之資訊安全的評量工具設計，介紹評量設計之系統需求、評量工具之操作程序與評量工具之分數計算方式。第二節將針對某 M 公司使用本論文所設計的評量工具作實證，並分析其實證結果。第三節將逐一說明 M 公司之企業資訊網站所遇到的風險因子與改善策略之建議。最後為 M 公司改善結果分析與改善前、後之比較。

一、評量工具之建置

本節主要介紹評量工具設計時所需之軟、硬體設備，以及詳細敘述開發評量工具時所使用的系統之原理和本論文實際運用的公司案例（黃淑慧 2003）。最後，我們會顯示本論文所設計的評量工具之操作畫面，並且提出弱點相關改善策略。

（一）評量工具設計之系統需求

本研究所開發之企業資訊網站平台之資訊安全的評量工具使用構環境如下：

根據本研究所提出的企業資訊網站平台之資訊安全的評估模式為基礎，並以微軟公司（Microsoft）新一代的程式開發環境.NET 架構（Framework）下進行企業資訊網站平台之資訊安全評量工具開發。

（二）評量工具之操作程序

依據本論文所推導的資訊網站之資訊安全評估之演算法，設計一套資訊網站

安全評量工具，而此評量工具主要是用來評估針對該架構之下的資訊網站之資訊安全。

（三）評量工具之量化計算方法

由於本研究之資訊安全範圍並未將硬體設備納入考量，故評量工具之計算公式是採取在一個企業資訊網站運行當中，當網站發生資訊安全危機時，該資訊安全因子之防護程度之量化計算分數乘以整體資安權重值如公式(3)，本研究之評量工具之量化計算分數如表 16。

資訊安全值=資安權重值×防護程度 (3)

表 16：評量工具之量化計算表

資安因子	防護程度 / 整體權重值	1 100% 很強	2 200% 強	3 300% 普通	4 400% 弱	5 500% 很弱
跨站腳本攻擊	0.0871	8.71	17.42	26.13	34.84	43.55
注入弱點	0.0756	7.56	15.13	22.69	30.25	37.82
不安全的物件參考	0.0462	4.62	9.24	13.87	18.49	23.11
身分驗證功能缺失	0.0386	3.86	7.72	11.57	15.43	19.29
未驗證的網路重新導向	0.0382	3.82	7.64	11.46	15.28	19.10
不安全的網路傳輸	0.0325	3.25	6.49	9.74	12.99	16.24
跨站冒名請求	0.0279	2.79	5.58	8.37	11.15	13.94
網站安全組態不當設定	0.0195	1.95	3.90	5.84	7.79	9.74
未加密的儲存設備	0.0168	1.68	3.36	5.04	6.72	8.40
SQL Server	0.0289	2.89	5.78	8.67	11.56	14.45
My SQL	0.0246	2.46	4.91	7.37	9.82	12.28
Oracle	0.0214	2.14	4.28	6.42	8.55	10.69
DB2	0.0131	1.31	2.61	3.92	5.23	6.53
Informix	0.0059	0.59	1.19	1.78	2.38	2.97
Sybase	0.0052	0.52	1.05	1.57	2.10	2.62
Microsoft Windows	0.1014	10.14	20.28	30.43	40.57	50.71
Linux	0.0763	7.63	15.27	22.90	30.54	38.17
UNIX	0.0526	5.26	10.52	15.77	21.03	26.29
專屬 OS	0.0301	3.01	6.03	9.04	12.06	15.07
Web browsers	0.0485	4.85	9.70	14.55	19.40	24.25

資安因子	防護程度 / 整體權重值	1 100% 很強	2 200% 強	3 300% 普通	4 400% 弱	5 500% 很弱
E-mail	0.0409	4.09	8.18	12.27	16.36	20.45
FTP	0.0264	2.64	5.29	7.93	10.57	13.21
Telnet	0.0232	2.32	4.63	6.95	9.27	11.58
Media Players	0.0145	1.45	2.90	4.34	5.79	7.24
Anti-virus Software	0.0125	1.25	2.50	3.75	5.00	6.24
Backup Software	0.0078	0.78	1.56	2.33	3.11	3.89
Office Software	0.0071	0.71	1.41	2.12	2.82	3.53
資料外洩	0.0413	4.13	8.26	12.39	16.52	20.65
人為操作不當	0.0250	2.50	5.00	7.50	10.01	12.51
SOP 流程疏失	0.0169	1.69	3.37	5.06	6.75	8.44
管理人員資訊技術不足	0.0136	1.36	2.71	4.07	5.43	6.79
資料誤用	0.0112	1.12	2.24	3.36	4.48	5.61
資料鍵入錯誤	0.0100	1.00	2.01	3.01	4.01	5.02

二、實證結果分析

本論文以某 M 商業銀行作實證案例，由南部某合會儲蓄公司改制而成。成立之初，資本額為舊台幣貳仟萬元，設有總公司及嘉義、新營、虎尾、北港等分公司，營業區域為雲嘉南縣市，並以投標式合會業務開始營運。民國 64 年 7 月 4 日我國銀行法公佈實施，規定合會儲蓄公司列為專業銀行，並自民國 67 年 1 月 1 日起奉准改制為「南部某中小企業銀行」於同年正式對外營業。於民國 71 年奉財政部證券管理委員會核准補辦公開發行，並於民國 72 年股票公開上市。

首先我們在 4 月 1 日時，請 M 商業銀行公司的資訊部門三位人員，使用本論文所設計的資訊網站評量工具來測試 M 公司資訊網站之資訊安全，其評量結果如圖 4。從結果顯示得知，此本案例經過評量工具進行計算評估後，網站資訊安全值為 277.72，對照於本論文所訂定的網站資訊安全等級標準，可得知 M 公司網站資訊安全等級為 C，可見其公司之資訊網站之資訊安全是需要進行改善的。

圖 4：改善前 M 公司資訊網站之評估結果

三、改善策略之建議與改善前後分析

本論文依據各種不同的資訊安全構面與資訊安全因子，提出了相對應的改善策略建議之範例，可以讓企業依照此改善策略之範例來對公司的資訊網站之資訊安全作改善。

根據本章第二節的結果分析，我們可以得知 M 公司的資訊網站存在了許多資訊安全，在此我們也對這些資訊安全因子提出了相對應的改善策略範例，以下我們就針對 M 公司所遇到的網站資訊安全因子加以分析。

（一）改善策略之建議

以下為本論文針對企業資訊網站之資訊安全因子，所提出的相關改善策略之建議，如表 18。

表 18：資訊安全因子的改善策略建議

	資訊安全因子	改善策略之建議
網頁應用構面	注入弱點	使用 Prepared Statements，使用 Stored Procedures、嚴密的檢查所有輸入值、使用過濾字串函數過濾非法的字元、控管資料庫及網站使用者帳號權限
	跨站腳本攻擊	檢查頁面輸入數值、輸出頁面做 Encoding 檢查、使用 Microsoft Anti-XSS Library
	身分驗證功能缺失	使用完善的 COOKIE / SESSION 保護機制、不允許外部 SESSION、登入及修改資訊頁面使用 SSL 加密、設定完善的 Timeout 機制、驗證密碼強度及密碼更換機制
	不安全的物件參考	避免將私密物件直接暴露給使用者、驗證所有物件是否為正確物件、使用 Index / Hash 等方法，而非直接讀取檔案
	跨站冒名請求	確保網站內沒有任何可供 XSS 攻擊的弱點、在 Input 欄位加上亂數產生的驗證編碼、在能使用高權限的頁面，重新驗證使用者、禁止使用 GET 參數傳遞防止快速散佈
	網站安全組態不當設定	軟體、作業系統是否都有更新到最新版本？不需要的帳號、頁面、服務、連接埠是否都有關閉？安全設定是否都完備？伺服器是否都有經過防火牆等設備保護？
	未加密的儲存設備	使用現有公認安全的加密演算法，減少使用已有弱點的演算法，例如 MD5 / SHA-1，甚至更簡單的加密法、安全的保存私鑰
	不安全的網路傳輸	盡可能的使用加密連線、Cookie 使用 Secure Flag、確認加密憑證是有效並符合 domain 的、後端連線也使用加密通道傳輸
	未驗證的網路重新導向	非必要時避免使用 Redirect 及 Forward、驗證導向位置及存取資源是合法的
資料庫構面	SQL Server	設定存取權限、選擇安全檢查模式
	Oracle	設定 Oracle NET 安全機制、Listener 加密、利用 Connect Manager 當做 FireWall、使用檔案加密
	My SQL	設定 phpMyAdmin 登入認證方式、設定資料庫管理者帳號、密碼

	資訊安全因子	改善策略之建議
資料庫構面	DB2	預設隔離等級、使用 Control Center 管理、權限設定
	Informix	權限設定、nformix 資料重組
	Sybase	權限設定、裝置組態設定、及裝置認證授權存取管理
作業系統構面	Microsoft Windows	Windows 防火牆設定、安全性層級設定，隱私權設定，自動更新設定、例外處理、連接埠設定
	Linux	防火牆設定、ACL 權限設定，帳號管理，取消不必要的服務、限制系統的出入、追蹤駭客的蹤跡
	UNIX	加強系統安全性以及微調防火牆、系統命令和配置檔來跟蹤入侵者的來源路徑、系統管理員要定期去觀察系統的變化、保護特殊的系統命令和系統配置檔以防止入侵者替換獲得修改系統的權利
	專屬 OS	管理人員可以依需求來設定作業系統之安全性
網路應用構面	Web browsers	安裝更強大的防毒軟體
	E-mail	使用收信軟體過濾信件
	Media Players	定期更新程式
	FTP	使用 Gateway Security Appliance，使用 SSL
	Telnet	防火牆應具備網路服務的轉送伺服器，使用 SSL
	Backup Software	使用付費版功能強大的備份軟體
	Anti-virus Software	隨時更新軟體及病毒碼，使用付費防毒軟體
	Office Software	隨時更新軟體，使用加密軟體
人為管理構面	資料外洩	使用監控軟體及保安軟體
	SOP 流程疏失	使用有效的 ERP 系統管理
	管理人員資訊技術不足	人員訓練及人員進用之評估
	人為操作不當	建立操作手冊及相關程序操作
	資料誤用	建立危機資訊溝通網路、警報系統
	資料鍵入錯誤	將公司流程電腦化，並加入 ERP 系統輔助使資料完整性，並使用審核機制與資料比對機制

（二）改善結果與分析

經由本論文所提出的評量工具，M 公司的資訊部門人員在第一次評量過後，並且透過相關的改善策略建議來改善公司的資訊網站。經過兩個月後，我們再請

M 公司的資訊部門三位人員再做一次評估，發現 M 公司的資訊網站之資訊安全值降低為 197.81、資訊安全等級為 D。

由於 M 公司透過本論文提出的改善策略建議後，已經將 Web 應用構面所存在的資訊安全因子之作出應有的改善。然而，除了將資料庫方面加強權限方面控管，另外也將提升作業系統之防火牆等級。在網路應用構面方面，M 公司以有採納本論文建議，除了將軟體安全性稍許提升，也考慮更換安全性更高的軟體。最後在人為管理構面方面，目前也正在對資料外洩、管理人員技術不足、人為操作不當資訊安全因子做出改善對策，例如：資料安全的控管、加強員工技術與操作方面的訓練等許多改善方式，不過這些都是需要長時間持續進行的，因此皆為正在改善中。然而，M 公司之企業資訊網站改善前資訊安全值較為高，經過改善後資訊安全值降低，其改善前、後分數比較表如 17。

表 17：改善前與改善後比較表

評估因子	改善前	改善後
注入弱點	37.82	30.25
跨站腳本攻擊	34.84	26.13
身分驗證功能缺失	15.43	11.57
不安全的物件參考	13.87	9.24
跨站冒名請求	8.37	5.58
網站安全組態不當設定	3.90	1.95
未加密的儲存設備	5.04	3.36
不安全的網路傳輸	6.49	3.25
未驗證的網路重新導向	11.46	7.64
SQL Server	11.56	8.67
Microsoft Windows	40.57	30.43
Web browsers	14.55	9.70
E-mail	16.36	12.27
Media Players	4.34	2.90
FTP	5.29	2.64
Telnet	4.63	2.32
Backup Software	2.33	1.56
Anti-virus Software	1.25	1.25
Office Software	1.41	0.71

評估因子	改善前	改善後
資料外洩	16.52	12.39
SOP 流程疏失	3.37	1.69
管理人員資訊技術不足	5.43	4.07
人為操作不當	7.50	5.00
資料誤用	3.36	2.24
資料鍵入錯誤	2.01	1.00
資訊安全總值	277.72	197.81

陸、結論

由於企業資訊網站與電子商務之應用已經越來越廣泛，因此，企業資訊網站之資訊安全已經是非常重要課題之一，而企業資訊網站之資訊安全並非單項資訊安全產品功能即可解決，必須整合相關之資訊安全技術以符合機密性、完整性、可用性和記錄性等特性。原則上，建置時亦須將相關資訊安全技術加以整合，以提供較完整且較健全之安全與信任的企業資訊網站環境。為了使資訊流通過程能夠保有安全性，我們設計了一套具有資訊安全性的資訊網站評估模式與其評量工具。本論文之具體研究成果及學術貢獻如下。

1. 首先，我們先參照了國際標準 ISO 27001 以及 ISMS 流程的制定，並整理 OWASP 與 SANS 組織所提出的網站資訊安全因子，然而透過專家問卷及 AHP 層級分析法評估，可以計算出專家問卷對於資訊網站系統安全之資訊安全因子之相對權重值與排序，並且以數值的形式，來表示每個資訊安全因子數值，依照數值的範圍，訂出各種不同資訊安全等級。
2. 依照資訊安全之評估模式，本論文設計出一套企業資訊網站之資訊安全的評量工具。
3. 利用本研究所設計之評量工具，對於現有企業資訊網站平台進行實證，並且分析其實證結果。
4. 透過個案實證，可以看出 M 公司之資安值從 277.72 降為 197.81，資訊安全等級也從 C 層級需要注意，降為 D 等級勉強接受。
5. 對於各種不同資訊安全等級之資訊安全因子，我們也提出了相關的改善策略建議，讓企業能夠對資訊網站之資訊安全所存在的資訊安全因子做出適當的改善，以確保企業資訊網的安全性。
6. 然而，Web-based 應用系統可利用本論文所提出的資訊網站之資訊安全的評估模式作為建置安全的企業資訊網站平台或其他電子商務系統參考模式。

誌謝

本論文承蒙兩位匿名審查委員之寶貴意見與悉心指正，使得本論文得已修正並更加完善，謹此致謝。

參考文獻

ISO 27001（2005），資訊安全管理系統－要求.（BSI, ISO 27001:Information Security Management Systems (ISMS) - Requirements.）

ISO/IEC 27005（2008），資訊安全風險管理標準.（BSI, ISO/IEC 27005 Information Security Risk Management Standard.）

陳俊德（2009），『數位學習網站系統資訊安全風險管理研究』，未出版碩士論文，華梵大學資訊管理學系，新北市。

林玉峰（2005），『網路攻擊與防護評比指標』，未出版碩士論文，樹德科技大學資訊管理研究所，高雄市。

翁宇能（2009），『應用 AHP 於資訊部門績效評估研究』，未出版碩士論文，國立中央大學資訊管理學系碩士在職專班，桃園縣。

施藍欣（2008），『知識移轉之資訊科技適化特質』，未出版碩士論文，國立高雄大學亞太工商管理學系，高雄市。

羅福枝（2005），『台灣資訊系統整合業工程人員績效評估之研究』，未出版碩士論文，世新大學資訊管理研究所碩士論文，台北市。

黃淑慧（2003），『應用模糊理論構建知識管理績效評估模式及系統開發之研究』，未出版碩士論文，大葉大學資訊管理學系，彰化市。

鄧振源、曾國雄（1989），『層級分析法的內涵特性與應用（上）』，*中國統計學報*，第二十七卷，第六期，頁 5-22。

韓慧林、王貴民、王振陽、劉庭維、鄭曳庭（2011），『應用失效模式與效應分析評估資訊安全管理系統之風險』，*國防雜誌*，第二十六卷，第六期，頁 107-122。

楊欣哲、彭勝寶（2013），『延伸型攻擊樹分析法以評估網站安全風險之研究』，*資訊管理學報*，第二十卷，第一期，頁 1-38。

OWASP TOP 10, Category: OWASP Top Ten Project, available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (accessed 25 March 2014).

SANS TOP 20, Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, available at http://www.sans.org/critical-security-controls/ (accessed 25 March 2014).

Cachia, E. and Micallef, M. (2007), 'A multi-tier, multi-role security framework for

e-commerce systems', *Proceedings of 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07)*, Tucson , USA, March 26-29, pp. 422-432.

Yang, C.H. and Wan, J.C. (2008), 'An approach to separating security concerns in e-commerce systems at the architecture level', *Proceedings of 2008 International Symposium on Electronic Commerce and Security (ISECS 2008)*, Guangzhou, China, August 3-5 , pp. 749-753.

Allen, J., Christie, A., Fithen, W., McHugh, J. & Pickel, J. (2000), *State of the practice of intrusion detection technologies*, (No. CMU/SEI-99-TR-028). Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., & Weippl, E. (2007), 'Information security fortification by ontological mapping of the ISO/IEC 27001 standard', *Proceedings of the Dependable Computing (PRDC 2007) 13th Pacific Rim International Symposium on*, Melbourne, Victoria, Australia, December 17-19 , pp. 381-388.

Barafort, B., Humbert, J.P. & Poggi, S. (2006), 'Information security management and ISO/IEC 15504: the link opportunity between security and quality', *Proceedings of the SPICE 2006 conference*, Luxembourg, May 4-5

Saaty, T.L. (1990), 'How to make a decision: the analytic hierarchy process', *European Journal of Operation Research*, Vol. 48, No. 1 , pp. 9-26.

Saaty, T.L. (1980), *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*, RWS Publications, Pittsburgh.

Likert, R. (1932), 'A technique for the measurement of attitudes', *Archives of Psychology*, Vol. 140, pp. 1-55.

附錄一：焦點座談－專家背景名單

座談專家	彭勝實	陳勇君	劉朝華
服務單位（現職）	永豐銀行資訊處副理	阿碼科技 / 行銷副總	友達科技股份有限公司 / 資深經理
工作經歷與資安相關工作經歷	1. 財金資訊公司安全審查委員 2. 永豐銀行資訊處資訊安全專員 3. 中華民國銀行公會金融業務電子化委員會資訊安全組委員	瑞百通資安股份有限公司、TWNIC 往安委員會委員、優易資訊副總、傑特科技副總、巨安資訊資安顧問、數聯資安顧問	交通部 WEB 應用系統原碼安全機制、國防部 WEB 應用系統原碼安全機制、國科會 WEB 應用系統原碼安全機制等等
主要專長	系統安全、資訊安全、電腦稽核	資訊安全、資安管理、網路安全、網站安全、資料庫安全	WEB 資訊安全應用與評估
相關證照	BS7799/ISO27001 Lead Auditor、TCSE	CISSP，ISO 27001 LA	N/A

附錄二：問卷調查－專家或學者背景名單

訪談專家	彭勝實	陳勇君	劉朝華	楊欣哲	謝明宏
服務單位（現職）	永豐銀行資訊處副理	阿碼科技 / 行銷副總	友達科技股份有限公司 / 資深經理	1. 東吳大學資訊管理學系專任教授 2. 中華民國資訊管理學會常務理事 3. 經濟部科技專案審查召集人 / 審查委員	銓聯資訊公司 / 系統部經理
工作經歷與資安相關工作經歷	1. 財金資訊公司安全審查委員 2. 永豐銀行資訊處資訊安全專員 3. 中華民國銀行公會金融業務電子化委員會資訊安全組委員	瑞百通資安股份有限公司、TWNIC 往安委員會委員、優易資訊副總、傑特科技副總、巨安資訊資安顧問、數聯資安顧問	交通部 WEB 應用系統原碼安全機制、國防部 WEB 應用系統原碼安全機制、國科會 WEB 應用系統原碼安全機制等等	1. 東吳大學專任教授兼系主任 2. 國立清華大學科技法律所兼任教授 3. 財團法人臺灣網路資訊中心網路安全委員會委員 4. 經緯電腦公司技術支援部 經理	資安講師；網路規劃架設
主要專長	系統安全、資訊安全、電腦稽核	資訊安全、資安管理、網路安全、網站安全、資料庫安全	WEB 資訊安全應用與評估	網路 / 雲端技術與應用、Web 應用系統設計、網路管理與安全、資訊管理	系統整合、網路管理
相關證照	BS7799 / ISO27001 Lead Auditor、TCSE	CISSP，ISO 27001 LA	N/A		TCSE