網路銀行資訊安全風險評鑑方法－以 ISO 27001 為基礎

徐淑如[1]　　林婉婷[2]
[1]國立嘉義大學資訊管理學系 slhsu@mail.ncyul.edu.tw
[2]國立嘉義大學行銷與運籌研究所

摘要

隨著資訊化時代的來臨，銀行紛紛架設專屬網站，設立網路銀行以提供多元化的金融商品與便利的服務，研究顯示資訊安全是阻礙消費者採用網路銀行服務最主要的原因。針對網路銀行資訊安全之控管，本研究以 ISO27001 訂定之風險因素為規範，結合失效模式與效應分析模型，提出一風險評量與排序方法，就網路銀行資訊安全風險因素之嚴重性、發生率與難檢度三個層面，計算風險優先數，據以衡量其威脅程度，研究中並透過個案案例驗證所提方法之可行性，期能提供網路銀行系統管理者分析資安風險因素控管優先順序方法之參考。

關鍵詞：網路銀行、資訊安全、風險評鑑、ISO 27001、失效模式與效應分析

網路銀行資訊安全風險評鑑方法－以 ISO 27001 為基礎

1. 緒論

隨著資訊化時代的來臨，顧客對金融服務需求型態也隨之改變，希望能以最快速便利的方式取得所需的商品及服務。為了滿足顧客的服務需求，架設網路銀行(以下簡稱網銀)，已成為銀行業發展多元化服務的重要策略。根據 104 市調中心(2009)針對台灣地區網路銀行及線上投資理財行為調查，約有六成的網友表示半年內使用過網銀，較 2008 年數據增加約 20%，使用網銀的網友中，有高達 92%表示未來將會繼續使用，未使用者中有 40%表示將考慮使用，顯示網銀使用者持續增加的趨勢。

網銀由於交易迅速，以及不受地點、時間限制之優勢，符合現今社會的需求。屏除不了解功能、申請流程麻煩與難以改變交易習慣等因素外，根據創市際市場研究顧問公司(2007)的調查，阻礙消費者使用網銀最主要的原因即是對交易安全的顧慮，Turkey (2009)亦指出安全性是阻礙網銀使用的主要因素。

我國對於網銀業務安全標準及設計是由財政部主管，內容包含交易面與管理面之安全需求及設計(財政部金融局，2000)，雖然為網銀系統之管理與設計提供了法律面的規範，然由於其各項服務高度仰賴資訊系統，隨著資訊技術變動或是因資訊系統的弱點或不當使用帶來營運的風險，例如：2004 年殺手(Sasser)病毒造成全台三分之一的郵局因工作站電腦當機影響金融業務的進行。根據美國聯邦調查局 FBI 與電腦安全協會 CSI 針對財星五百大企業、金融組織、政府單位、醫療院所，以及大學院校等 538 個單位調查發現，於 2000 年至 2001 年間資訊安全的相關破壞事件，有 85%的組織遭受過資訊安全(以下簡稱資安)破壞，因而產生財務或生產力的損失，其中 70%源自網際網路。面對日益複雜的網路攻擊手法，企業開始重視資安管理，惟大部分對資安的認知仍停留在病毒與駭客入侵的議題上，對於資訊資產的保護以及系統管理安全的知識仍相當不足。

ISO27001 資訊安全管理系統規範為英國標準協會(British Standards Institution, BSI)於 2005 制定的資安管理規範，是公認最完整的資通安全架構及認證標準，最早源於 BSI 發布之 BS7799 標準，用以評估檢討組織之資安作業，提供組織進行資訊風險的評估與處理，防範意外的發生及對組織的衝擊(BSI, 2002)。行政院國家資通安全會報採用 BS7799，要求如：國土安全、能源設施、金融服務等列入資安等級 A 級的單位必須於 2004 年以前通過此項認證(行政院國家資通安全會報，2004)。ISO27001 標準之風險管理流程首先是界定組織安全的需求及管理範圍，以進行資訊資產的鑑別，進而實施系統風險的評鑑，根據評鑑結果訂定風險管理的優先順序，以能在管控成本與降低風險效益中取得平衡。因此，應用 ISO27001 的意義之一，是在組織資源及管理時間有限的情況下，分析可能造成危害的潛在因素，找出威脅資訊安全的重大風險，優先配置資源進行控管，以將風險對組織資訊資產的危害降至最低。

因應日益複雜的網路交易環境，企業日益意識到資訊安全管理的重要性，目前國內已有不少組織導入 ISO27001 資安管理系統，規範資訊資產風險之評估與控管。對於高度仰賴資訊網路運作的金融業而言，更是其關切的重要課題，國內如華信、兆豐金控、花旗、第一、建華、中華郵政、國泰世華、新光、台新等銀行紛紛加入 ISO27001 認證，

建立組織資安系統化的架構。惟目前針對金融業建置 ISO27001 資訊安全管理系統的研究仍不多見，且偏向認證導入效應的探討，例如黃明達與曾淑惠(2003)以 BS7799 為基礎，比較本國銀行及外商銀行資訊安全的運用狀況；賴怡伶(2004)基於 BS7799 提出銀行支付系統的資訊安全管理模式；Granova and Eloff (2004)針對網路銀行身分竊取問題，以 BS7799 為基礎提出控管標準；Chau (2005)探討 ISO27001 運用於金融業的法律問題；吳振昀(2006)比較金融服務業間導入資訊安全管理機制前後資訊安全衝擊之差異；以及陳志誠等(2009)以國內某銀行為個案，結合 ISO27001 與美國國家技術標準局(NIST)之「資訊科技系統風險管理指導」進行資訊資產風險的分級與控管。

雖然 ISO27001 針對組織資安風險來源提供了相當完整的參考架構，亦以規劃、執行、查核及處置(PDCA)進行週期性的風險管理，規劃流程中更訂定組織應進行「定義風險評鑑系統之方法」、「辨識風險」、「評鑑風險」等工作要項，然而對於各項風險因素效應的評量，並未提供明確與周延的評估方法，需藉助風險分析理論之量化或質化評估方法進行，此外，ISO27001 規範之風險因素涵蓋安全政策、組織安全、資產分類等十一項領域，各領域包含多項細部因子(BSI, 2002)，在組織資源有限情況下，有必要就各風險因子評量結果予以分級，作為控管優先順序的依據。

有關風險效應的評估方法方面，目前實務上以失效模式與效應分析法(Failure Mode and Effects Analysis, FMEA)的應用最受矚目，FMEA 為應用於產品開發、設計、製造、維修的方法，針對特定產品或系統發生的問題，就問題的嚴重性(Severity)、發生頻率(Occurrence)、及難檢度(Detect)等指標，計算風險優先數(Risk Priority Number, RPN)，依據重點改善原則，針對 RPN 較高者，列為優先的改善標的，並實際執行改善的方案，以提高產品的品質及可靠性(林哲宏、鍾國章，2008)。FMEA 是以失效為焦點，著重於設計或生產階段可能的缺失、損害或事故，用以避免失效發生或是降低失效造成之負面效應，是提高系統安全性與穩定度相當有效的工具(Tay and Lim, 2006; Sharma et al., 2007)。目前 FMEA 已經成為 ISO-9000 與 QS-9000 品質體系的主要工具之一，最近亦有研究探討應用 FMEA 於如顧客稽核系統(曾俊傑等，2008)、電子商務(Linton, 2003)等服務失效風險的情況。

據此，針對網銀資安風險之評量與分級，本文基於 ISO27001 定義之風險因素，結合 FMEA 方法，提出一風險評量方法，就各資安風險因素之嚴重性、發生率與難檢度三個層面，計算風險優先數，據以衡量其威脅程度，其中難檢度為檢視網銀現行的資安控管能力，對於銀行檢視目前風險控管措施有相當的幫助。研究中並透過一個案案例驗證所提方法之可行性，提供網銀系統管理者分析資安風險因素控管順序方法之參考。

2. 文獻探討

投稿論文以未曾發表之研究或實務性論文為限，其方程式、表格、圖片規定如下。

2.1 網路銀行

根據財政部對網路銀行的定義，係指由客戶端電腦經網際網路與銀行電腦進行連線，無須親赴銀 行櫃台，即可直接取得各項金融服務(財政部金融局全球資訊網，2009)。網路銀行的基本功能包括個人帳戶查詢、線上轉帳、繳款交易、外匯及貿易服務等各項

銀行業務、理財試算功能、買賣共同基金，以及其他各金融機構依特色與功能提供的服務項目等(行政院金融監督管理委員會，2002)，其優點包括持續 24 小時不間斷的服務時間，提供消費者方便和有效的方式管理財務狀況(Tan and Teo, 2000)，減少實體投資與交易成本(Pant and Hsu, 1996)；不僅打破時間、距離的限制、傳遞最即時的信息(Orr, 1997)，亦提供民眾更多元的服務(Bomil and Ingoo, 2002)。

就電子商務的發展，安全性是影響使用者從事網路交易的最主要因素之一，網銀的使用亦面臨相同情況。網銀從純粹提供金融產品與服務介紹，進展成為銀行與顧客間的交流管道(如：電子郵件、對帳單、個人資料更新等)，其後更執行如匯款、轉帳等實際金融交易，在此一進展過程中，顧客最關心的是網銀服務的安全性(盧志敏，2004 年)。目前已有不少研究關注網路銀行安全與隱私等相關議題，如：Cranor et al.(1999)藉由實證研究證實隱私問題是阻礙網路銀行使用的重要原因；沈宗奇(2000)針對國內網路銀行消費者行為分析亦發現，消費者選擇網路銀行最重視的層面是安全性；Ioannis(2008)探討各文化在網路銀行風險溝通與安全系統運作的重要性；林南宏、蔡佳穎(2009)研究發現四成的民眾擔心使用網路銀行將造成個人資料外洩，提昇網站的安全性將有助於提高消費者的使用意願。

2.2 ISO27001 資訊安全認證制度

目前最新國際認證資安管理系統版本為 2005 年的 ISO17799:2005(Code of practice for information security management)及 ISO27001:2005(Information security management systems (ISMS)- requirements)。ISO17799:2005 目標是設立產業最佳的資安管理準則；而 ISO27001:2005 則詳述 IT 安全應用與稽核應遵循的架構：

1. ISO17799:2005 資安管理作業要點

此為資訊安全管理之國際共通語言，提供廣泛性的資訊安全管理準則，作為現行資安規範之最佳指導方針，其並不作為驗證標準，內容共有 15 個章節，前 4 章簡介資訊安全管理適用範圍及相關名詞定義與風險評鑑的作法，後 11 章說明安全政策、組織安全、資產分類與控制、人員安全、實體與環境安全、通信與作業管理、存取控制、資訊安全事故管理、系統開發之維護、營運持續管理及遵循性等 11 類資訊安全管理控制作業領域規範。

2. ISO27001:2005 資訊安全管理系統要求

ISO27001:2005 根據 ISO17799:2005 提供組織全面性資安管理系統建置基準與稽核遵循的模式，依據個別組織的要求，落實執 行資安管理，並作為正式評鑑與驗證的標準。內容規範包含 11 項控管領域、39 項控管目標及 133 項控管方法，提供組織實施與控管措施選擇之參考依據。

由於資安管理系統的應用為一項持續性的工作，企業組織導入後尚須依規劃、執行、查核及處置的品質管理流程，進行週期性持續的風險管理，以因應可能的改變。BSI 於 2006 年進一步提出 BS7799-3:2006，定義風險管理程序為進行風險辨識及評估等風險評鑑流程後進行風險處理，依據 ISO IEC Guide 73:2002 的定義，風險評鑑(risk assessment)為風險分析與風險評估的整體流程，其中風險分析(risk analysis)為有系統地使用資訊，辨識風險來源，以預估風險；風險評估(risk evaluation)則是將所預估的風險與已知的風

險標準進行比較，以決定風險的重要性。BS7799-3 的處理過程中仍遵循 PDCA 循環，使可接受的風險水準能隨著每次的循環逐步達到更高的要求。BS7799-3 風險評鑑包括 12 項步驟，並以風險發生的可能性及所造成的後果二項因子做為評量風險等級的基礎。

目前對於 BS7799/ISO27001 應用的探討已擴及多個領域，例如：葉相妤(2002)以 BS7799 為標準來檢視各醫療院所之資訊安全管理現況；劉永禮(2002)利用 BS7799 之規範，建立組織資訊安全之認知，並就機密性、整體性及可用性三項指標，建立資訊安全風險評估方式；王俊雄(2002)交叉比對分析 BS7799 國際資通訊安全規範與現行警察資通安全管理規定；曾淑惠(2002)採用問卷調查法，探討本國銀行及外商銀行在 BS7799 的運用狀況；Carrison et al. (2003)運用 BS7799 探討醫學影像存檔與通訊系統；黃士銘等(2006)調查國內石化產業的資訊安全議題及現況，分析影響石化產業導入資安管理機制的關鍵因素；許雪蓮(2006)以 ISO27001 調查軍事單位人員對導入 ISO27001 的看法，提供國軍建立資安管理制度參考；以及 Shuchih (2006)探討影響 ISO27001 實施有效性之組織因素。

2.3 失效模式與效應分析(FMEA)

FMEA 是一項風險項目分析技術，找出可能的失效/故障模式，並預測其產生的影響及意義，有助於提高系統或產品安全性與穩定度 (Sharma et al., 2007)。FMEA 是以造成失效之風險項目為焦點，著重生產或設計階段可能發生的事故、缺失、損害，用以避免失效發生或降低失效造成之負面效應(Tay and Lim, 2006)。

FMEA 針對特定產品思考可能發生的問題，藉由嚴重性、發生率、難檢度三項指標，計算 RPN 以評斷其風險等級，做為改善優先順序的依據，計算方式為：RPN=嚴重性×發生率×難檢度，其中，嚴重性為問題的嚴重程度，評估潛在風險項目對於其他要素、顧客或系統的影響；發生率代表問題的發生率，定義特定原因或機制發生的可能性；難檢度衡量問題能被檢測出的機率，評估目前系統偵測潛在原因發生的能力，此三項指標一般由專家進行評定，RPN 數值越高代表失效可能性越高(蔡介元，2002)。

FMEA 具有：原理簡單易於了解；以潛在造成失效的風險項目為出發點，有助於組織定義、迴避及降低風險帶來的負面影響；可應用於產品設計或者是製程階段等優點。一般性而言，FMEA 可適用於產品設計、生產製造、品管驗收等各個階段。由於 FMEA 的應用日趨廣泛，更吸引許多研究者的注意，例如：Carbone and Tippett (2004)藉由個案研究法，以 FMEA 為基礎，提出一專案風險管理流程與評估方法；Teng et al. (2006)探討供應鏈應用 FMEA 協同改善產品設計、品質的議題；楊錦洲等(2006)應用 FMEA 於醫藥物流作業流程，以個案探討的方式對個案公司中各單位主管進行訪談，並重新塑造一套適合於醫藥品的物流作業流程；Welborn (2007)將 FMEA 應用於外包風險評估，以一家美國公司 RadioShack Store Fixture (RSSF)為案例，協助管理者進行評量和決策；林哲宏與鍾國章(2008)將 FMEA 應用於電子化服務品質之建立，深度訪談 3G 手機產業中不同部門的資深人員及專家，提出幾項行動通訊業重大的風險項目，做為業者進行改善的參考；曾俊傑等(2008)發展並驗證一顧客稽核缺失管理系統，透過 FMEA 評核所提列的矯正及預防措施的有效性；莊情惠與莊秀文(2009)運用 FMEA 分析評估化學治療給藥的潛在風險。

3.研究模式

根據 BS7799-3 之規範，組織資安風險評鑑流程包含鑑別威脅、評估威脅、預估損失、計算風險係數、鑑別與評估控制措施等步驟，其中在鑑別威脅部份，本研究以 ISO27001 資安管理作業要點訂定之 133 項控制項目為架構，作為網銀鑑別資安威脅之風險來源；在評估威脅、預估損失、計算風險係數、分析脆弱點、鑑別與評估控制措施部份，BS7799-3 主要是以風險發生的可能性及造成的後果二項為評量風險威脅的基礎，之後考量控制該項風險之成本，藉以權衡處置該項風險之優先性，由於 BS7799-3 對上列步驟並未提供具體之執行方法，此外，如何整合風險威脅與控制成本進行權衡，亦缺乏理論的規範，針對此一問題，本研究採用 FMEA 法，結合嚴重性、發生率與難檢度三項構面，計算網銀資安風險優先數，其中嚴重性係評估資安風險因素可能產生的損失；發生率為估計造成資訊資產傷害風險因素發生的可能性；難檢度為評估目前控制機制發現潛在資安風險因素的能力，反映目前偵測、控制該項資安威脅來源的能力，藉由風險優先數整合風險發生的可能性、後果與控制機制三項因子，衡量各項資安風險因素之威脅程度。

綜上所述，有關網銀資訊安全風險評鑑方法之架構如圖 3-1 所示，共包含鑑別資安威脅；定義資安威脅嚴重性、發生率、難檢度的評估標準；評估威脅嚴重性；評估威脅發生率；評估威脅難檢度；以及計算風險優先數，各步驟主要內容與採用方法說明如下：

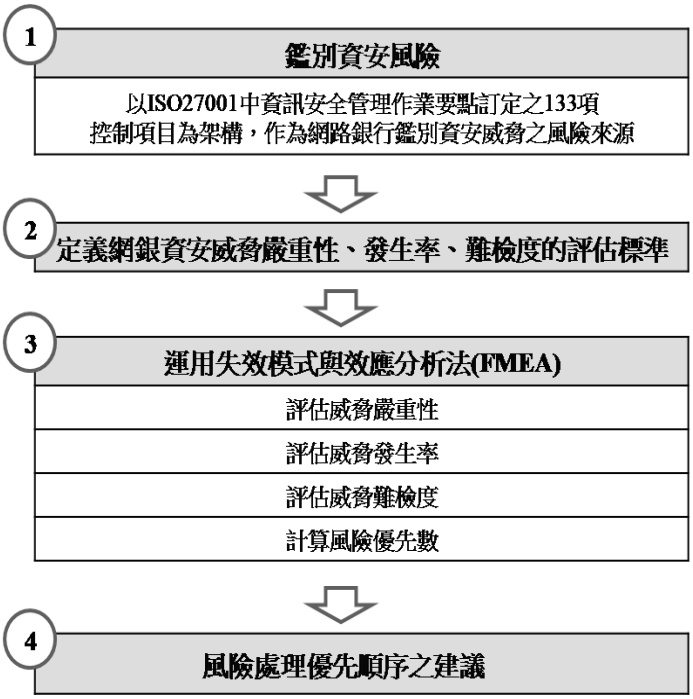

圖 3- 1　研究架構圖

1. 鑑別資安威脅

本研究以 ISO27001 中資訊安全管理作業要點訂定之 133 項控制項目為架構，作為網路銀行鑑別資安威脅之風險來源。

2. 定義網銀資安威脅嚴重性、發生率、難檢度的評估標準

此步驟針對 FMEA 的嚴重性、發生率與難檢度三項風險衡量指標，經專家評估修正

後，重新定義適合網路銀行實際應用之評定標準，結果如表 3-1、表 3-2、表 3-3 所示。

表 3- 1　嚴重性評分標準

效果	標準	等級
危險無警告	當一個潛在風險項目影響安全和(或)涉及與網路銀行規定不符時，非常高的嚴重性等級，失效會在無警告的情況下發生性	10
危險	當一個潛在風險項目影響安全和(或)涉及與網路銀行規定不符時，很高的嚴重性等級，失效會在有警告的情況下發生	9
甚高	系統完全報廢，功能無法運作，喪失基本功能	8
高	系統部份報廢，系統功能尚能運作，但功能下降，造成顧客不滿	7
中等	部份系統組成報廢，系統功能仍可運作，但方便性降低，造成顧客不滿	6
低	系統功能可運作，但某些功能下降，造成顧客些許不滿	5
甚低	系統某一功能不合要求，大多數顧客會注意到此缺陷	4
很小	系統某一功能不合要求，一般顧客可注意到此缺陷	3
微乎其微	系統某一功能不合要求，敏銳的顧客會注意到此缺陷	2
無	為顧客無法發現的缺陷	1

表 3- 2　發生率評分標準

失效機率	可能的失效率	等級
甚高：失效幾乎不可避免	≧1/2 1/3	10 9
高：反覆發生的失效	1/8 1/20	8 7
中等：偶爾發生的失效	1/80 1/400 1/2000	6 5 4
低：相對很少發生的失效	1/15000 1/150000	3 2
極低：失效不太可能	≦1/1500000	1

表 3- 3　難檢度評分標準參考表

效果	標準	等級
幾乎不可能	現在沒有已知的控制以檢測出該項風險	10
幾乎微乎其微	現行的控制檢測出該項風險的可能性極其微乎其微	9
絕少	現行的控制檢測出該項風險的可能性絕少	8
甚低	現行的控制檢測出該項風險的可能性甚低	7
低	現行的控制檢測出該項風險的可能性較低	6

中等	現行的控制檢測出該項風險的可能性中等	5
適度的高	現行的控制檢測出該項風險的可能性不低	4
高	現行的控制檢測出該項風險的可能性較高	3
甚高	現行的控制幾乎可以確定能檢測出該項風險	2
幾乎可確定	現行控制檢測不出該項風險的可能性微乎其微	1

資料來源：修改自吳貴彬與陳相如(2003)

3. 運用失效模式與效應分析法

延續上一步驟，運用失效模式與效應分析法，就嚴重性、發生率與難檢度三項構面，依下列法則計算 RPN 值；RPN 值 =嚴重性×發生率×難檢度。對應原先 BS7799-3 之評量基礎，FMEA 納入難檢度指標，評估組織發現風險威脅的能力為控制成本不可或缺的重要指標，除了有助於評估風險威脅外，亦有助於風險威脅與控制成本兩者間之權衡。

4. 風險處理優先順序之建議

此步驟乃依據前述專家群體意見的彙整結果，排定網路銀行風險處理之優先順序。

4.個案應用與分析

4.1個案背景介紹

個案銀行創設於 1905 年，迄今逾 100 年，總行起初設於彰化，為銀行發軔之始，在全台 25 個縣市設有 171 個服務據點，其中包括 6 個海外分行，分別為紐約、洛杉磯、東京、倫敦、香港、新加坡分行與大陸昆山代表處。該銀行於 2004 年設立網路銀行，隸屬於資訊處之下，依顧客類型區分為企金與個人金融兩部分，提供的線上服務包括網路 ATM，帳戶餘額與交易明細查詢、轉帳、密碼變更，十大常用繳費；協助政府各單位稅收繳交；亦提供資金帳戶管理、融資管理、貿易管理等服務。銀行採用 SSL128 位元安全加密機制，確保客戶使用時一切資料傳輸皆經加密處理；以及採用 VeriSign 提供的延伸驗證(EV) SSL 認證，確保交易網站的安全性。個案銀行於 2007 年取得並落實 ISO27001 資安認證，銀行內部針對網路銀行的推行，頒布資安相關的管理規範，並制定資訊處理安全手冊以確保資訊系統及服務之機密性、完整性及可用性。

4.2ISO27001-FMEA 之應用

個案進行是由銀行網路銀行企金及消金業務專責資安人員各一名參與評量作業，首先由研究人員解釋 FMEA 之意義與三項風險衡量指標之定義，回答評估人員對於三項指標評定標準認定之問題。二位評估人員皆具備參與 ISO27001 導入經驗，對於各題項風險項目之意涵，並未有太多的疑問與解釋需求。

4.3個案銀行風險分析結果

評估人員完成個案網路銀行企金與消金風險評量問卷後，首先檢視問卷填答內容之完整性，其後針對各題項之嚴重性、發生率與難檢度分數，計算三者乘積以產生 RPN，之後依各題項 RPN 進行排序，據以產生本個案企金與消金之資安風險處理優先排序。由表 4-1 與表 4-2 之 RPN 分佈顯示，企金部分 RPN 值超過 200 分僅 19 項，包括「要求使用者使用通行碼(RPN=450)」、「具機密性的系統有專屬(隔離)的電腦作業環境(RPN=450)」、「已使用密碼控制措施保護重要資訊措施(RPN=450)」、「進　行密鑰管理，以適當地支援組織對加密技術的使用(RPN=450)」、「採取控制措施以保護軟體開發委外

工作的安全(RPN=420)」等；而消金部分 RPN 值超過 200 分有 15 項，包括「進行密鑰管理，以適當地支援組織對加密技術的使用(RPN=540)」、「鑑定應用程式實施控制訊息，以確保訊息真實性和內容完整性(RPN=450)」、「應用系統資料輸出經過確認，確保所儲存資訊之處理程序正確」、「所有的員工、承包商和第三方用戶，注意並主動報告系統或資訊服務中已發現或疑似的安全弱點(RPN=420)」、「限制及控管公用程式之使用(RPN=400)」、「即時獲得組織資訊系統技術　漏洞的資訊，評估組織對此類技術漏洞的保護方式，並立即採取適當的改善措施，以降低漏洞對組織產生的風險(RPN=360)」等。

表 4-1　個案銀行企金 RPN 分佈

RPN 範圍	項目個數
401~500	6
301~400	2
201~300	11
101~200	21
1~100	93

表 4-2　個案銀行消金 RPN 分佈圖

RPN 範圍	項目個數
501~600	1
401~500	3
301~400	3
201~300	8
101~200	19
1~100	99

在提供 RPN 分佈資料予個案銀行二位評估人員並徵詢其意見後，皆同意以嚴重性、發生率與難檢度 6 分(超過中間值)之乘積(RPN=216)以上者視為高風險項目，並依此進一步針對高 RPN 風險項目進行分析，分別列出企金部分 19 項與消金部分 15 項之網銀資安高度風險項目，如表 4-3 與表 4-4 所示。分析表 4-3 所列企金資訊安全首要風險項目排名，其中，以「要求使用者使用通行碼」、「具機密性的系統有專屬(隔離)的電腦作業環境」、「已使用密碼控制措施保護重要資訊措施」與「進　行密鑰管理，以適當地支援組織對加密技術的使用」為影響網路銀行安全最大之威脅因素，顯示密碼控制措施是個案銀行須優先處理的課題。

表 4-4 列示個案銀行消金資訊安全風險項目的排名，其中，以「進行密鑰管理，以適當地支援組織對加密技術的使用」為最影響網路銀行安全最大之威脅因素，顯示資料加密是該銀行維護消費金融資訊安全的首要工作。

總括個案銀行在企金 19 項與消金 15 項之高 RPN 值風險項目中，共有 5 項相同，分別為「設備在報廢或再次使用前，將附屬之資訊清除」、「使用合適的密碼管　理系統，

提供互動式、有效的設施以確保密碼的安全性及可用性」、「進　行密鑰管理，以適當地支援組織對加密技術的使用」、「採取控制措施以保護軟體開發委外工作的安全」與「即時獲得組織資訊系統技術漏洞的資訊，評估組織對此類技術漏洞的保護方式，並立即採取適當的改善措施，以降低漏洞對組織產生的風險」，顯示個案銀行應特別注意「資訊系統的獲得、開發與維護」項目之控管。

表 4-3 個案網路銀行企金資訊安全首要風險項目

題項	項目名稱	RPN	排名
78	要求使用者使用通行碼	450	1
95	具機密性的系統有專屬(隔離)的電腦作業環境	450	1
103	已使用密碼控制措施保護重要資訊措施	450	1
104	進行密鑰管理，以適當地支援組織對加密技術的使用	450	1
112	採取控制措施以保護軟體開發委外工作的安全	420	5
113	即時獲得組織資訊系統技術漏洞的資訊，評估組織對此類技術漏洞的保護方式，並立即採取適當的改善措施，以降低漏洞對組織產生的風險	405	6
81	使用者只能直接存取明確准許使用之服務	360	7
82	控管使用者電腦服務之存取路徑	360	7
80	可移動式電腦使用完畢，將相關重要內容清空，以防止未經授權存取	252	9
126	組織重要紀錄予以保護，以防止遺失、毀損及偽造	252	9
128	禁止非授權的用戶不當使用資訊處理設備	252	9
89	所有使用者具有專屬的使用者識別序號，以便追蹤責任歸屬	240	12
90	使用合適的密碼管理系統，提供互動式、有效的設施以確保密碼的安全性及可用性	240	12
92	高風險之應用系統，設定連線時間限制，以多一層安全保護	240	12
127	根據相關法令採取控制措施保護個人資訊	240	12
11	對於外部組織存取公司的資訊處理設施時，可能發生的風險進行確認，並在同意存取前實 施適當的控制措施	216	16
25	違反公司資訊安全政策與程序之員工，能確實依規定予以懲罰處理	216	16
39	設備在報廢或再次使用前，將附屬之資訊清除	216	16
40	公司之設備未經授權允許，不得擅自帶離工作場所	216	16

表 4-4 個案網路銀行消金資訊安全首要風險項目

題項	項目名稱	RPN	排名
104	進行密鑰管理，以適當地支援組織對加密技術的使用	540	1

101	鑑定應用程式實施控制訊息，以確保訊息真實性和內容完整性	450	2
102	應用系統資料輸出經過確認，確保所儲存資訊之處理程序正確	450	2
115	所有的員工、承包商和第三方用戶，注意並主動報告系統或資訊服務中已發現或疑似的安全弱點	420	4
91	限制及控管公用程式之使用	400	5
113	即時獲得組織資訊系統技術漏洞的資訊，評估組織對此類技術漏洞的保護方式，並立即採取適當的改善措施，以降低漏洞對組織產生的風險	360	6
111	防止資訊洩漏的機會	320	7
39	設備在報廢或再次使用前，將附屬之資訊清除	280	8
106	測試資料予以保護及控制	256	9
84	控制遠端系統過濾合理的存取	252	10
112	採取控制措施以保護軟體開發委外工作的安全	252	10
100	系統內有確認檢查機制，以偵知所處理資料之塗改	250	12
90	使用合適的密碼管理系統，提供互動式、有效的設施以確保密碼的安全性及可用性	240	13
98	新系統或現有系統提升之營運需求中，詳述各項控制措施之要求	225	14
108	採取正式變更管制程序，以嚴格控制變更作業之實施	216	15

另針對ISO27001-FMEA法之易用性與有用性等接受度之評量。首先，針對ISO27001結合FMEA應用的易用性，由於個案銀行於2007年已導入ISO27001，因此企金及消金業務評估人員，皆認為此風險項目是容易瞭解的，而在評估嚴重性、發生率與難檢度上亦無困難，並且認為整體上是容易使用的。而在方法的有用性上，已導入ISO27001之個案銀行之評估人員均給予本法正面的評價，認為藉由本法的採用納入了難檢度指標的考量，有助於檢視網路銀行現行的資安控管能力，評估可能的控管弱點，對於銀行修正風險控管的措施有相當的幫助。最後，在導入與使用意願上，個案銀行的二位評估人員皆同意，若公司採用此法均願意落實此項評估方法。

5.結論與建議

網路銀行所面臨的風險相當廣泛，要全面歸納整理各風險項目實屬困難，有鑑於此本研究以國際認證標準 ISO27001 資訊安全管理作業要點訂定之 133 項控制項目為架構，作為網路銀行鑑別資安威脅之風險來源，降低分析人員歸納與辨識風險因素的困難。

針對 133 項資安風險項目，個案評估人員由於具有 ISO27001 導入經驗，因此認為是容易瞭解的，二位評估人員在風險項目的認知尚稱一致，風險威脅因素主要在「資訊系統得獲得、開發與維護」領域。ISO27001 原以各風險發生的可能性及其所造成的後果二項為評量風險威脅的基礎，本研究結合 FMEA 的應用，將 FMEA 中難檢度列為一新衡量指標，在風險評鑑中，難檢度衡量風險發生後能被檢測發現的機會，反映現行組織對風險控制的有效性，風險項目的難檢度越高，代表失效產生時，現行的控制機制很

難發現系統失效的發生，例如，某種病毒入侵組織資訊系統時，系統能立即發現予以阻隔的能力，因此，錯失即時處理之時機，可能造成系統因此失效而持續損失。相較於只考慮嚴重性與發生率，加入難檢度的考量，部份風險項目排名有的顯著差異，例如：企金案例中，風險項目「建立資訊之處理及儲存程序，防止資訊被不當揭露或誤用」，原先排名為 66，採用 FMEA 法後，因難檢度為 9，排名提升為 20；而「違反公司資訊安全政策與程序之員工，能確實依規定予以懲罰處理」此項風險，消金原先排名為 119，採用 FMEA 法後，因難檢度達 8 分，使得排名提升為 77 等情況即是。此外，就排名差異之變化程度，使用相對測度值變異係數(Coefficient of Variance)進行衡量，變異係數為樣本標準差除以樣本平均數，變異係數愈大者表示資料間的差異愈大，結果顯示企金變異係數為 0.771，消金變異係數為 0.816，意味納入難檢度，相較於企金部門，網銀消金之資安風險因素控管優先順序產生較顯著的改變。

針對 ISO27001-FMEA 法風險評估的有用性，二位評估人員均給予本方法正面的評價，認為藉由本法的採用，可以有系統的辨識風險項目，進行風險威脅程度評估，此外，評估人員亦認為納入難檢度指標的考量，有助於檢視網路銀行現行的資安控管能力，評估可能的控管弱點，對於銀行修正風險控管的措施有相當的幫助與啟發。

另就 133 項風險項目 RPN 平均數，企金部分以「存取控制」、「資訊系統得獲得、開發與維護」與「資訊安全事故管理」構面分數較高；消金部分為「資訊系統得獲得、開發與維護」與「資訊安全事故管理」構面，綜合而言，「資訊系統獲得、開發與維護」與「資訊安全事故管理」為該網銀資安主要之威脅層面，建議企業在此二部份優先進行改善。本研究所列出的網銀資安首要風險項目數中，個案企金 19 項與消金 15 項多屬於「資訊系統的獲得、開發與維護」與「存取控制」二層面，推論可能是公司已導入 ISO27001，人員在風險項目的看法及認知上較具一致性。

在 133 項的風險項目排序中，個案銀行企金與消金的排序上差異較大的項目為「對於可攜式電腦儲存裝置(隨身碟等)訂有相關控制管理措施」、「要求使用者使用通行碼」與「測試資料予以保護及控制」。其中「對於可攜式電腦儲存裝置(隨身碟等)訂有相關控制管理措施」(企金名次為 20，消金名次為 118)，主要的差異來自嚴重性衡量指標(企金為 9，消金為 5)；而「要求使用者使用通行碼」項目(企金名次為 1，消金名次為 104)，主要的差異亦來自嚴重性指標(企金為 10，消金為 5)，企金評估人員表示資料授權存取與密碼保護等作業在企金業務部份格外嚴格的，因為其涉及的金額與層級較高，失效所造成的影響也較為嚴重；而「測試資料予以保護及控制」項目(企金名次為 105，消金名次為 9)，消金評估人員則表示以其個人經驗與認知測試資料的保護很容易忽略，在測試的環境當中的正式資料容易忽略遮蔽，因此在發生率的部分差異較大。

本研究以網路銀行的資訊安全風險管理為研究對象，後續研究可以本研究方法為基礎，探討其它產業或企業資訊安全風險評估的議題。此外，本研究將各資安風險項目視為獨立成因，但許多問題的產生往往存在著前因後果，評定最須優先處理的風險項目可能是由另一個優先權較低的風險項目所引發，因此風險項目間可能存在因果關係，後續研究者可就此狀況探討風險項目嚴重性、發生率與難檢度之評估方法。

參考文獻

1. 王俊雄 (2002),「警政資通安全管理政策之研究」,國立中央警察大學資訊管理研究所未出版碩士論文。

2. 吳振昀 (2006),「金融服務業導入資訊安全管理機制影響之研究」,國立台北科技大學商業自動化與管理研究所未出版碩士論文。

3. 吳貴彬、陳相如 (2003),「失效模式與效應分析之應用」,中華民國品質學會第 39 屆年會暨第 9 屆全國品質管理研討會。

4. 沈宗奇 (2000),「台灣地區網路銀行利益區隔與消費者行為之研究」,國立東華大學國際企業管理研究所碩士論文。

5. 林南宏、蔡佳穎 (2009),「創新擴散理論對網路銀行接受度的影響-科技接受模式的應用」,2009 台灣科技大學管理新思維學術研討會發表論文。

6. 林哲宏、鍾國章 (2008),「應用失效模式與效應分析於電子化服務品質之建立-以 3G 行動通訊產業為例」,運籌管理評論,第三卷,第一期,pp.47-58。

7. 財政部金融局 (2000),「金融機構辦理電子銀行業務安全控管作業基準」。

9. 莊情惠、莊秀文 (2009),「化學治療給藥之失效模式與效應分析」,護理雜誌,第 56 卷,第 4 期,pp.62-70。

9. 許雪蓮 (2006),「以 ISO27001 為基礎評估軍事單位資訊安全環境之研究:以國軍 M 單位為例」,私立大同大學資訊經營研究所未出版碩士論文。

10. 陳志誠、林淑瓊、李興漢、許派立 (2009),「資訊資產分類與風險評鑑之研究－以銀行業為例」,資訊管理學報,第 16 卷,第 3 期,pp.55-84。

11. 曾俊傑、童超塵、廖乃毅 (2008),「運用品質機能展開及失效模式與效應分析-建構顧客稽核管理系統」,品質學報,第 15 卷,第 5 期,pp.313-322。

12. 曾淑惠 (2002),「以 ISO27001 為基礎評估銀行業的資訊安全環境」,私立淡江大學資訊管理研究所未出版碩士論文。

13. 黃士銘、張碩毅、蘇耿弘 (2006),「企業導入 ISO27001 資訊安全管理系統之關鍵成功因素－以石化產業為例」,資訊管理學報,第 13 卷,第 2 期,pp.171-192。

14. 黃明達、曾淑惠 (2003),「以 ISO27001 為基礎評估銀行業的資訊安全環境」,資訊管理展望,第 5 卷,第 2 期,pp.31-50。

15. 楊錦洲、陳建誠、陳百盛 (2006),「建立醫藥物流作業流程 FMEA 模式」,中華民國品質學會第四十二屆年會。

16. 葉相妤 (2002)，「運用 ISO27001 檢測醫療院所資訊安全管理作業文件之研究」，國立陽明大學衛生資訊與決策研究所未出版碩士論文。

17. 劉永禮 (2002)，「以 ISO27001 資訊安全管理規範建構組織資訊安全風險管理模式之研究」，私立元智大學工業工程與管理研究所未出版碩士論文。

18. 蔡介元、許盛堡、陳麗君 (2002)，「建構一個 QFD 與 FMEA 之同步工程整合架構」，中華民國品質學會第 38 屆年會暨第 8 屆全國品質管理研討會。

19. 盧志敏 (2004)，「網路銀行的發展與影響」，中央銀行季刊第二十三卷第一期。

20. 賴怡伶 (2004)，「以 ISO27001 為基導入銀行支付系統資訊安全模式之研究」，私立輔仁大學資訊管理研究所未出版碩士論文。

21. Bomil S. and Ingoo H. (2002), “Effect of trust on customer acceptance of Internet banking,” Electronic Commerce Research and Applications, 1(3-4), pp. 247–263.

22. British Standards Institution. (2002), Information security management systems-part2: Specification with guidance for use.

23. BSI. (2005), BS 7799-1 Information Security Management-Part 1：Code of Practice for Information Security Management, London.

24. BSI. (2005), BS 7799-2 Information Security Management-Part 2：Specification for Information Security Management, London.

25. BSI. (2006), ISO27001 Information Security Management Systems. Guidelines for Information Security Risk Management.

26. Carbone, T.A. and Tippett, D.D. (2004), “Project Risk Management Using the Project Risk FMEA,” Engineering Management Journal, 16(4), pp. 28-35.

27. Cranor, I.F., Reagle, J. and Ackerman, M.S. (1999), “Beyond concern: understanding net users’ attitudes about online privacy.” Technical report, TR 99.4.3, AT&T Labs-Research, available at: www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm.

28. Carrison, K.S., Tong, K. H., Fung, H.Y., Huang, K.K. (2003), “Implementation of ISO17799 and ISO27001 in picture archiving and communication system: local experience in implementation of ISO27001 standard,” International Congress Series, 1256(2003), pp. 311-318.

29. Chau, J. (2005), “Skimming the technical and legal aspects of ISO27001 can give a false sense of security,” Computer Fraud & Security, 2005(9), pp. 8-10.

30. Granova, A. and Eloff, J. (2004), “Online banking and identity theft: who carries the risk?” Computer Fraud & Security, 2004(11), pp. 7-11.

31. Ioannis, V. K., Christos, M.. (2008), “Internet banking security in the contexts of goal setting, culture and risk communication,” International Journal of Risk Assessment and Management, 10(3), pp. 186-205.

32. Linton, J. (2003), “Facing the Challenges of Service Automation: An Enabler for E-commerce and Productivity Gain in Traditional Services,” IEEE Transactions on Engineering Management, 50(4), pp. 478-484.

33. Orr, B. (1997), “How to get your bank on the World Wide Web,” ABA Banking Journal, 88(4), pp. 44-54.

34. Pant,S. and Hsu, C. (1996), “Business on the web: strategies and economics,” Computer Networks and ISDN Systems, 28(7-11), pp. 1481-1492.

35. Sharma, R.K., Kumar, D. and Kumar, P. (2007), “Fuzzy Decision Support System (FDSS) for Conducting FMEA,” Journal of the Institution of Engineers Mechanical Engineering Division, 88(3), pp. 39-44.

36. Shuchih-Ernest, C. and Chienta-Bruce, H. (2006), “Organizational factors to the effectiveness of implementing information security management,” Industrial Management & Data Systems, 106(3), pp. 345-361.

37. Tan, M. and Teo, T.S.H. (2000), “Factors influencing the adoption of Internet banking,” Journal of the Association for Information Systems, 1(5), pp. 1-42.

38. Tay, K.M. and Lim, C.P. (2006), “Fuzzy FMEA with a Guided Rules Reduction System for Prioritization of Failures,” International Journal of Quality & Reliability Management, 23(8), pp. 1047-1066.

39. Teng, S.G., Ho, S.M., Shumar, D. and Liu, P.C. (2006), “Implementing FMEA in a Collaborative Supply Chain Environment,” International Journal of Quality & Reliability Management, 23(2), pp. 179-196.

40. Welborn, C. (2007), “Using FMEA To Assess Outsourcing Risk”, Quality Progress, 40(8), pp. 17-21.

41. 104 市調中心 (2009)，「台灣地區網路銀行及線上投資理財行為研究報告」，http://www.104ad.com.tw/article_detail.jsp?id=613。

42. ISO27001Home, http://www.dnv.com/searchresult/index.asp?query=ISO27001.

43. NIST. (2002), “ International Standard ISO/IEC 17799: 2000 Code of Practice for Information Security Management, ” http://www.thefreelibrary.com/Information+security+management+best+practice+based+on+ISO%2FIEC+17799%3B-a0134256186。

44. 行政院金融監督管理委員會全球資訊網 (2002),「我國銀行電子化政策相關議題」, http://oldwww.fsc.gov.tw/fp.aspx?icuItem=30829。

45. 行政院國家資通安全會報 (2004),「建立我國通資訊基礎建設安全機制計畫-94 年至 97 年」, http://www.pthg.gov.tw/CmsFile/ 200742694854234.pdf。

46. 財政部金融局全球資訊網 (2009),「個人電腦業務及網路銀行業務服務契約範本」, http://www.mof.gov.tw/mp.asp?mp=1。

47. 創市際市場研究顧問公司 (2007),「三成 金融網友使用網路服務，近五成股票族線上下單」, http://www.insightxplorer.com/news/news_01_26_07.html。

A Method of Information Security Risk Assessment for Internet Banking- Based on ISO 27001

Shu-Lu Hsu[1] Wan-Ting Lin [2]

[1] Department of Management Information Systems,
National Chiayi University, Taiwan, slhsu@mail.ncyu.edu.tw

[2] Graduate Institute of Marketing and Logistics Management
National Chiayi University

Abstract

This study proposes a risk assessment method for internet banking information security. This study uses ISO27001 risk factors and FMEA. Three measures are considered: the probability of failure occurrence, the impact or severity of the failure, and the capacity to detect failure before it occurs. The multiplication of these measures generates the RPN. According to RPN, we can distinguish different extents of risky menace.

Keywords: internet banking, information security, risk assessment, ISO 27001, FMEA