國立政治大學資訊管理學系

碩士學位論文

指導教授：林我聰 博士

雲端服務風險評估模式建立之研究

A Study on Developing A Cloud Service Risk Assessment Model

研究生：羅邵晏

中華民國一零二年一月

致謝

謝謝我林我聰老師這些年來不厭其煩的指導我，我也從林老師身上學到很多，包括供應鏈管理的知識、做研究的方法、做人做事的方法、還有老師最強調的邏輯概念，這些都是能夠一生受用無窮的能力。在老師的教導下，我從原本安於做一個「資訊技術人」啟發我成為真正「資管人」的更多可能性，套一句老師的話「很多問題到最後都不是技術的問題，而是人的問題」，這樣的概念也在我的研究中得到部分應證。接下來要感謝幫我填寫問卷的所有主管、和不參與研究也耐心回應我的收件者，雖然我的問卷並不是很好填，也收到一份回應不太好的無效問卷，但還大部分人還是耐心地幫助我完成研究，讓我試誤學習到很多問卷設計和回收的技巧。還要謝的還有同學、學弟妹、學長姐、和朋友們透過聊天討論給我建議、感謝口試委員在百忙中抽空前來審查我的論文、系辦助教協助我處理學業相關事項。最後最重要的是九十度鞠躬感謝母親大人這些年不求回報的支持我。

這些年來我在政大學習到很多，也改變我許多，不論是與研究相關的事、其他領域的知識、或是非學業的事，希望未來能學以致用才不會辜負所有人的幫助和支持。

摘要

「雲端運算」(Cloud Computing)及其相關應用服務受到業界相當重視。同時各國政府也相繼推出國家型計劃發展雲端運算產業。然而許多文獻告訴我們，雲端運算在資訊安全議題上也需要被重視。在雲端運算架構下的資訊安全又與過去有些許不同，值得被提出來研究。歐洲網路與資訊安全機構(European Network and Information Security Agency, ENISA)在 2009 年已經提出一份雲端服務風險評估報告(CCSRA, Cloud Computing Security Risk Assessment)，此份報告也被推出業界第一套雲端服務風險標準(CCSK, Certificate of Cloud Security Knowledge)的雲端安全聯盟(CSA, Cloud Security Alliance)所引用。這份評估報告已經相當完整定義各風險和其前因後果，但卻沒有完整的量化模式供組織進行量化評估、或預測整個雲端服務風險系統運作。因此本研究目的如下：1.建立一個量化模式，預測雲端服務風險相關風險，供企業主及早採取因應措施。2.以皮爾森相關係數法(Pearson Correlation Coefficient)分析各個風險、弱點、和資產間因果影響程度，讓組織在分配資源時作為參考。

關鍵字：雲端運算、雲端服務風險、風險評估、服務商評選、皮爾森相關

Abstract

“Cloud Computing” and its application services are considered important by industries. Governments have also launched plans to develop the cloud computing industry. However, the literature tells us that cloud computing security issues also need to be noticed. Security issues in the cloud computing architecture are different from those in traditional information system, so they are worth to be studied. In2009, European Network and Information Security Agency(ENISA) has announced a report named "Cloud Computing Security Risk Assessment", and this report was referenced by Cloud Security Alliance(CSA). The report is quite complete for the definition of each risk, its causes and effects. But there does not exist a complete quantitative model for the organization to assess or predict its cloud service risk. Therefore, the purposes of this study are as follows: 1. developing a cloud service risk assessment model to predict cloud service risks, 2. use Pearson Correlation Coefficient to analyze the impact between risks, vulnerabilities and assets for allocation of resources.

Keywords: Cloud Computing, Cloud Service Risk, Risk Assessment, Service Provider Selection, Pearson Correlation

目錄

圖目錄

表目錄

第一章、緒論

雲端運算(Cloud Computing)以風險管理議題最為重要，以下分別以背景、動機、目的說明本研究欲探討之議題及重要性。

1.1 研究背景

「雲端運算」及其相關應用服務受到業界相當重視。同時各國政府也相繼推出國家型計劃發展雲端運算產業。各國政府也相繼推出國家型計劃發展雲端運算產業。而雲端運算作為一種趨勢，在文獻中也可以略窺一二：「許多觀察家認為雲端運算代表下一代的伺服器運算。(Rosenthal et.al., 2010)」「目前透過網路來取得需要的資源或是應用服務已成為主流的趨勢，而行動通訊的普及，將促使雲端服務的應用更為多樣化。(蔡一郎, 2010)」「正由於雲端運算可以較少資源提供更多服務，各國都將雲端視為重要的 IT 技術。(林育震, 2010)」「雲端運算允許高度彈性的運算應用程式、儲存、和平台，在政府的資訊科技策略中越來越重要。(Paquette et.al., 2010)」

然而雲端運算真是如此完美嗎？許多文獻告訴我們，雲端運算除了有許多好處外，在資訊安全議題上也需要被重視：「儘管雲端運算擁有更彈性、敏捷、降低成本、易於備援等好處，安全性卻是一大隱憂。(林育震, 2010)」「決策標準被需要超越簡單的金錢成本，要包含降低風險、增加彈性和可擴展性、並保護機構的其他系統。(Rosenthal et al., 2010)」「雖然使用雲端運算被報導有很多好處，但雲端運算技術的執行、管理、和使用上仍然具有相當大的風險。(Paquette et al., 2010)」「資訊科技(IT)對供應鏈管理(SCM)的效能和效率產生重大影響…相關領域包含雲端運算和軟體即服務(SaaS)模式也是未來的研究方向，尤其資訊安全與線上儲存可能是重要的。(Schoenherr, 2009)」

另外過去資訊安全議題已經被研究多年，但在雲端運算架構下的資訊安全又有些許不同處，值得被提出來研究。林育震(2010)提到：「雲端服務風險和傳統 IT 基礎架構安全的最大不同，是前者共用大規模的基礎設施。同一組運算資源上來自不同公司的使用者交互存取。由於雲端的動態和瞬間變化特性，加上用戶希望不斷達到負載平衡和優化效能、能源、可用性，和其他服務水準協議（Service Level Agreement, SLA）的關注項目，問題變得更複雜，也提高錯誤組態和惡意行為的發生率。」

1.2 研究動機

現在我們知道了雲端運算作為資訊科技趨勢，其資訊安全議題特別需要被重視，而且雲端運算架構和傳統資訊系統架構不同造成資訊安全風險也不盡相同，需要被謹慎管理、重新評估。在這方面歐洲網路與資訊安全機構(European Network and Information Security Agency, ENISA)在 2009 年已經提出一份名為雲端服務風險評估(Cloud Computing Security Risk Assessment, CCSRA)的報告，此份報告也被推出業界第一套雲端服務風險標準(Certificate of Cloud Security Knowledge, CCSK)的雲端安全聯盟(Cloud Security Alliance, CSA)所引用。在這份報告裡面清楚定義了 35 個雲端運算架構下的風險(Risks)、53 個弱點(Vulnerabilities)、23 個可能受影響的資產(assets)、各個資產重要性、還有各風險的發生率和影響、並和過去傳統資訊系統架構做比較。這份評估報告已經相當完整定義各風險和其前因後果，但卻沒有完整的量化模式供組織進行量化評估、或預測整個雲端服務風險系統運作。

1.3 研究目的

因此本研究目的如下：

一.建立一個量化模式，只要針對各個弱點進行評估就可以預測出各個風險事故(peril)造成的影響，進而算出總體風險分數、建立風險矩陣。讓組織在選擇服務商、及分配資源時有所依據。

二.以皮爾森相關法(Pearson correlation)分析各個風險、弱點、和資產間因果影響程度，讓組織在分配資源時作為參考。

第二章、文獻探討

爲瞭解雲端運算資訊安全風險管理議題，本章將會分別介紹雲端運算、風險管理、和雲端運算的風險管理。

2.1 雲端服務模式

2.1.1 雲端運算的定義

在正式開始談雲端服務風險前，我們要先探討何謂雲端運算？Yusuf et.al.(2011)認為「『雲端運算』基本概念要回到 1960 年代 John McCarthy 認為的『運算能力某天可能會被組織起來變成一種公共事業』(這個比喻幾乎符合所有現代雲端運算的特徵，包括彈性供給、公用事業式的供應、 線上作業、無限供應的感覺)。...而首次在學術上使用雲端運算一詞的是 1997 年的 Ramnath Chellappa 教授。」Ramnath Chellappa & Gupta(2002)表示「Chellappa 描述的『雲端運算』(cloud-computing)是一個動態的運算框架，運算範圍由技術、經濟、地區、和資訊安全需求以及基礎服務提供者決定。」美國商務部標準與技術研究所(NIST, 2011)提到更明確的雲端運算定義是「一個具有方便性、能夠依需求網路存取結構化運算資源的模式(例如：網路、伺服器、儲存裝置、應用程式、和服務)，這些資源可以藉由極小的管理負擔或與雲端提供者的互動快速分配和釋放。(NIST, 2009)」Vaquero et.al.(2009)認為雲端運算「是一個能夠簡單使用和存取虛擬化資源(例如：硬體、發展平台、服務)的大池子。這些資源可以藉由被重複動態配置應付易變化的負載需求，以允許資源使用最佳化。而這池資源的利用方式就是一種典型的使用者付費模式，這種模式也同時具有令基礎架構提供者(Infrastructure Provider)擔保客製化服務保證協定(SLAs)的意義。」

綜合以上描述。雲端運算從技術上來看是一個動態運算框架，此框架把各種虛擬化資源(如：運算能力、儲存空間、記憶體、應用程式、服務)儲存在一個大池子中，並快速釋放和配置給使用者應付易變化的需求、最佳化資源使用。從服務觀點來看雲端運算是一種使用者付費模式，令使用者透過網路取得所需資源，用多少付多少，就像是水電一樣的公用事業。

2.1.2 雲端運算的服務模式

在傳統上組織資訊系統從基礎架構(硬體設備、儲存空間、網路、運算處理器...)、系統發展和執行環境(資料庫、中介軟體、發展套件、執行架構...)、還有應用軟體系統(CRM/ERP/HR、商業流程...)都由組

織自己一手包辦，而雲端運算服務模式依照外包程度不同(服務商提供資源不同)又可分為三種類，根據 IBM 在 Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security 紅皮書(2009)中所提及，分別為 SaaS、PaaS、IaaS(如圖 2-1)：

一.架構即服務(Infrastructure as a Service , IaaS)

提供顧客應付處理器、儲存體、網路、或其他基本運算資源需求的能力，並允許顧客部署和隨心所欲執行任何軟體(包含作業系統和應用程式)。(Zissis & Lekkas, 2011;Yoo ,2011)而在技術上是把虛擬機器(virtual machines ,VMs)依照需求大小快速且簡單的分配給顧客。(Vaquero et.al., 2011)

二.平台即服務(Platform as a Service , PaaS)

提供顧客部署自行創建或從外部獲取的應用程式，而此應用程式使用服務商支援的程式語言或工具建造在雲端架構上。(Zissis & Lekkas, 2011)終端使用者可以控制和設計應用程式，但無法接觸到基礎架構。(Yoo, 2011)

三.軟體即服務(Software as a Service, SaaS)

提供顧客線上使用在雲端架構上執行的應用程式，這個應用程式能夠在各種不同的輕型客戶端裝置(thin client)上被使用，例如：Web-based mail。(Zissis & Lekkas, 2011)且終端使用者不能控制應用程式設計、伺服器、網路、或儲存架構。(Yoo, 2011)

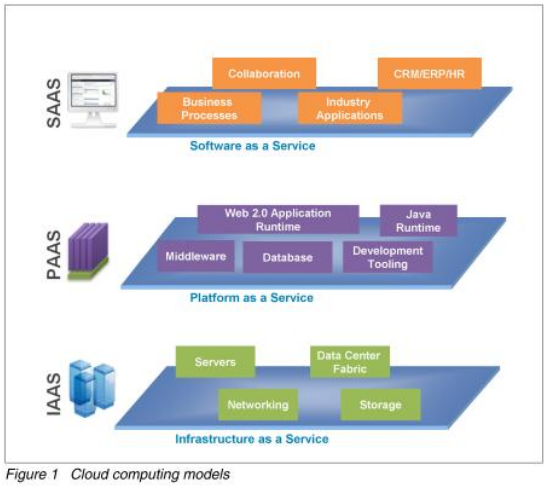


Figure 1 Cloud computing models

圖 2-1. 雲端運算的三種服務模式

資料來源：IBM(2009), 'Red Book ─ Cloud Security Guidance ─ IBM Recommendations for the Implementation of Cloud Security', IBM

而美國商務部標準與技術研究所發展出更完整的雲端架構。整個架構包含雲端消費者、雲端稽核、雲端提供者、雲端代理商、和雲端負載

者等五大塊，其中雲端提供者裡又包含安全、隱私、服務管理、資源抽取與控制層、和實體資源層，而原本的 SaaS、PaaS、IaaS 則縮到雲端提供者的服務層級內。(如圖 2-2)

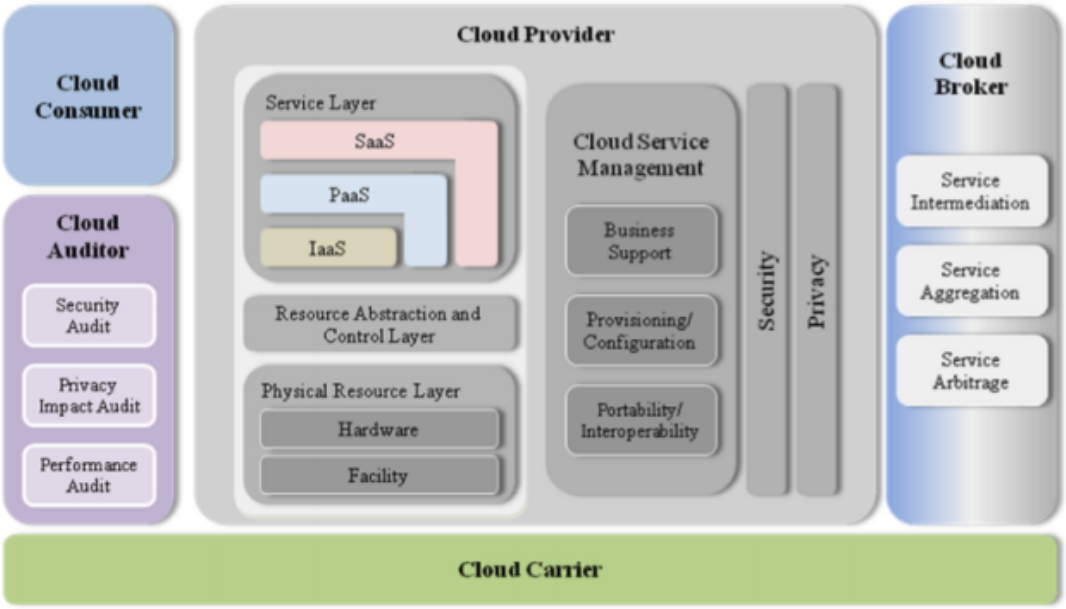


圖 2-2. 美國商務部標準與技術研究所提出的雲端架構
資料來源：NIST SAJACC and BUC Working Groups(2011), 'NIST US Government Cloud Computing Technology Roadmap Volume III - Technical Considerations for USG Cloud Computer Deployment Decisions', National Institute of Standards and Technology

從以上文獻中可以歸納出這 Laas、SaaS、PaaS 三種服務模式已經是美國政府與業界共同認可的主要雲端服務提供模式。

2.2 風險管理之概念與程序

2.2.1 風險的定義

管理學大師 Peter Drucker 說過：「經營企業若想完全除去風險是不可能的。」所以說必須正視風險的存在，在事前或事後加以管理才能把風險對組織的影響減到最小。為了有效管理風險(Risk Management)，首先要瞭解什麼是風險(Risk)。張春雄等人(2003)引用三位不同領域學者的定義「加州大學財務學教授 Philippe Jorion 對於風險的定義為：對資產或負債價值非預期結果之波動性；美國經濟學者 Knight,F.認為風險為可測定之不確定性；保險學者 Willet,A.解釋風險為某種不幸是發生與否之不確定性；Snider,H.W.稱風險為損失之不確定性。綜上所述，

所謂風險者即某種損失發生之不確定性。」陳瑞&周林毅(2007)更明確歸納了風險(Risk)的三種意義「某種損失發生的不確定性、不幸事故發生的可能性、一事件可能產生不同結果的變異。」從以上敘述可以歸納出風險是一種不確定性(Uncertainty)，不確定是否會發生、不確定發生後的狀況是否造成損失、或不確定發生後損失的嚴重度，但通常會更注重有損失(Loss)的狀況，因此「風險(Risk)」一辭便常常和「不幸」、「事故」、「災」等字詞一起出現。只有損失而無獲利可能的風險稱做純風險(pure risk)。「因此風險具有損失(Loss)和不確定性(Uncertainty)兩項構成要素。」(張春雄等人,2003)「而世界標準組織(ISO)在ISO31000:2009 中使用風險的定義是『對目標的不確定性影響(effect of uncertainty on objectives)』。」(Purdy, 2010)

2.2.2 風險管理的步驟

有了風險的概念，再來看看風險該如何被管理。根據張春雄等人(2003)整理的程序，共分為風險認定、風險評估、對策選擇、決策實行、績效評估與回饋五個步驟(圖 2-3)：

一.風險辨識(Risk Identification)：辨識各種風險的存在，並隨時注意新風險形成。

二.風險衡量(Risk Measurement)：辨識出有哪些風險後，要評估各個風險的兩要素(也就是不確定性和損失)，通常會用各個過去的發生頻率和造成損失的嚴重程度來衡量。

三.對策選擇(Selection of techniques)：接下來要針對各個風險選擇事前措施及事後處理的對策(制定風險管理政策)，事前措施不外乎是避免(將風險降為零)、預防(降低發生率)、減抑(降低損失)、分散風險、風險轉移(例如買保險)、或是選擇保留。

四.決策實行(Implementation of decisions)：想好該怎樣處理各個風險後要實際執行。

五.績效評估(Evaluation of performance)：評估上述步驟是否確實以及成效如何，並修正政策更符合現實需要。

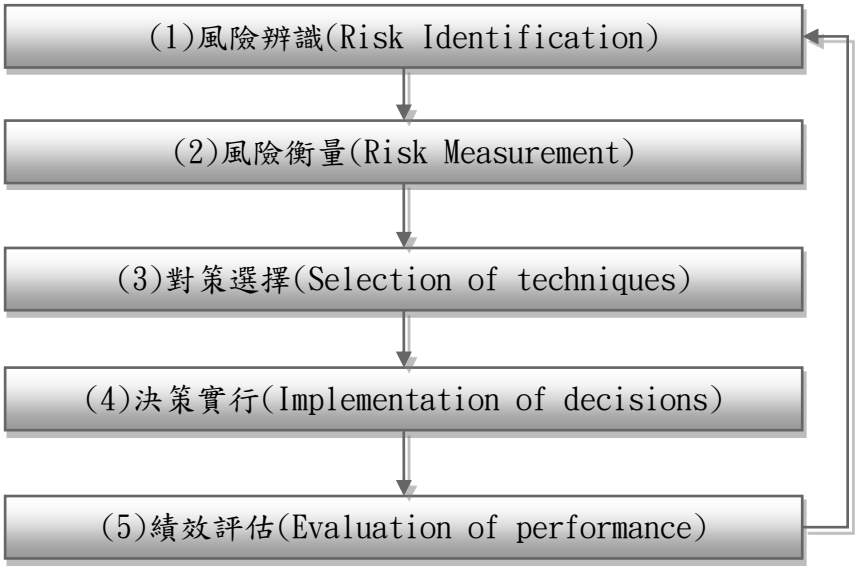


圖 2-3.風險管理之步驟
資料來源：簡化自張春雄等人，2003，風險管理，吉田出版

2.3 資訊安全風險管理概念與目標

風險管理有一些專有名詞，在各領域裡的風險管理概念上大同小異，只是差在一些慣用語、或描述的詳細程度不同...等細節而已。因此資訊資產的風險管理(資訊安全)也不例外。

2.3.1 風險管理概念

Mayer 等人(2007)整理了十五篇文獻包含風險管理標準(Risk management standards)、資訊安全標準(Security related standards)、安全風險管理方法(Security risk management methods)、軟體工程安全框架(SE security frameworks)中的概念和用詞，如下表所示總共有五個概念(表 2-1)：

表 2-1.十五篇文獻之風險管理概念與用詞比較表

文獻	概念(1)	概念(2)	概念(3)	概念(4)	概念(5)
ISO/IEC Guide 73	Risk	Event	Consequence	-	-
AS/NZS 4360	Risk	Event	Consequence	-	-
ISO/IEC 27001	Risk	-	Impact	Threat	Vulnerability
ISO/IEC 13335	Risk	-	Harm	Threat	Vulnerability
Common Criteria	Risk	Threat	Consequence	-	Vulnerability
NIST 800-27 NIST 800-30	Risk	-	Impact	Threat	Vulnerability
EBIOS	Risk	Threat	Impact	-	Vulnerability
MEHARI	Risk Risk scenario	Cause	Consequence	-	-
OCTAVE	Risk	-	Impact Consequence	Threat	Vulnerability
CRAMM	Risk	-	Loss	Threat	Vulnerability
CORAS	Risk	-	Consequence incident	Threat scenario	Vulnerability
Haley et al. Moffett and Nuseibeh	Risk	-	Impact	Threat	Vulnerability
Firesmith	Safety Risk Security Risk	-	Impact	Hazard Threat	Vulnerability

資料來源:繪製自 N.Mayer, P.Heymans, R.Matulevičius(2007), 'Design of a Modelling Language for Information System Security Risk Management', *Proceedings of the 1st International Conference on Research Challenges in Information Science(RCIS 2007),* Ouarzazate, Morocco, April

一.風險(Risk)：指「一個威脅(Threat)和至少一個弱點(Vulnerability)並導致一或多個資產(Asset)受到影響(Impact)。」這整件事情。例如：黑客(Cracker)入侵並偷走會員資料,造成商譽資產(Asset)受影響(Impact)。這整件事情叫做一個風險。

二.導致風險的原因(Cause of the risk)：風險事件會產生是因為「有某一個威脅(Threat)利用至少一個弱點(Vulnerability)。」例如：黑客(Cracker)會入侵的原因(Cause)是因為他利用了作業系統的弱點(Vulnerability)植入木馬程式。

三.影響(Impact):風險的潛在負面結果,可能會令資產(Asset)受到傷害。例如：受到黑客(Cracker)入侵竊取個資後所損失的商譽資產(Asset)。

四.威脅(Threat)：潛在的攻擊或風險事件，能利用一或多個弱點(Vulnerability)令資產(Asset)受到傷害。例如：黑客(Cracker)入侵這件事情就是一個風險。

五.弱點(Vulnerability)：一或多個資訊資產(Asset)具有對於資安方面脆弱(Weakness)或瑕疵(Flaw)的特徵。可能會被威脅(Threat)利用並導致故意或非故意的風險事故。例如：作業系統的漏洞可以被偷偷放進木馬程式。

整個關係如圖 2-4：

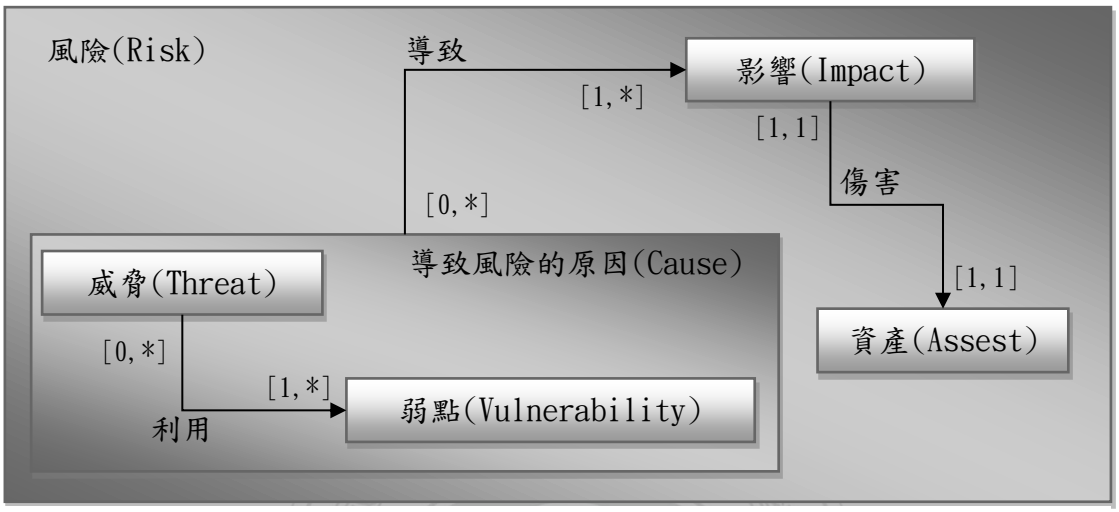


圖 2-4. 資訊安全各主要名詞概念圖

資料來源：N.Mayer, P.Heymans, R.Matulevičius(2007), 'Design of a Modelling Language for Information System Security Risk Management', *Proceedings of the 1st International Conference on Research Challenges in Information Science(RCIS 2007)*, Ouarzazate, Morocco, April

六.資產(Assest):「一般被定義為任何對組織有價值需要被保護的東西。而組織資訊或流程需要符合一些原則，以保護這些資產。這些屬性包含保密性(confidentiality)、完整性(integrity)、以及可用性(availability)。(ISO/IEC 13335-1:2004)」Mayer 等人(2007)。

2.3.2 受保護資產應該符合的準則：

我們都說關鍵資產應該受到保護，但資訊資產不是實體資產，資訊安全也和人身安全不同，不只是讓他活著就好。要讓資訊資產符合哪些原則才算是保護得好，各家門派也各有異同。

除了 Mayer 等人(2007)提到「受保護資產應該要符合保密性(confidentiality)、完整性(integrity)、以及可用性(availability)。(ISO/IEC 13335-1:2004)」是基本的三項原則外。歐洲成立的 CORAS 專案發展一套方法和工具支持模式基礎(Model-Base)的資訊安全風險評估框架系統，「CORAS 特別強調資訊安全包含所有定義、達成、和維持機密性

(confidentiality)、完整性(integrity)、可用性(availability)、不可否認性(non-repudiation)、有責性(accountability)、可稽核性(authenticity)、和可靠性(reliability) (ISO/IEC TR 13335-1:2001)」Yannis C. Stamatiou 等人(2002)。而這七個資訊安全基本準則說明如下(Avizienis et.al., 2000)：

一.機密性(confidentiality)：拒絕未被授權的資訊被揭露。

二.完整性(integrity)：拒絕不合法的系統狀態變更。

三.可用性(availability)：隨時準備提供正確服務。

四.不可否認性(non-repudiation)：訊息發送者和接受者身份資訊的完整且可用性。

五.有責性(accountability)：執行某項操作，操作者的身分資訊要符合可用性和完整性。

六.可稽核性(authenticity)：一個訊息的內容、來源和其他可能資訊(像是發送時間)應該要符合完整性。

七.可靠性(reliability)：持續提供正確服務。

2.4 雲端服務風險

2.4.1 雲端服務風險

從使用者角度來看，雲端運算服務模式最令人擔心的是他過於依賴網路、而且所有資訊通通放在別人家裡。一旦網路出了問題便無法工作，服務商出錯使用者的資料便受到威脅。從技術面來看，過去資訊安全存在的問題在雲端上同樣存在，而且還因為商業模式不同及技術匯流例如常伴隨雲端管理模式一起出現的虛擬化技術導入而更加複雜(虛擬化技術可能讓不同使用者共同使用同一組實體資源)。也有可能傳統資訊架構已經存在的安全問題發生率及影響提高或降低，而需要被重新評估。

Rosenthal 等人(2010)指出把資料儲存在雲端上可能會有以下類別風險：(1)安全技術管理問題(使用者如何確保雲內每台機器都安全、管理者如何確認每一個使用者的虛擬機器都安全、雲端管理機制該處理什麼人才能存取什麼資料...)；(2)因為駭客產生的風險(多租貸問題、安全保護的範圍...)；(3)非技術外包風險(和廠商間的商業糾紛或服務終止(包括破產)、某台虛擬機發生違法時會懲罰到誰、服務商員工監守自盜...)。

在國際組織方面，例如：美國國家研究院標準與科技研究所(National Institute of Standards and Technology, NIST)、Intel 為首的業界資訊安全聯盟(PCI)、歐盟網路與資訊安全機構(European Network and Information Security Agency, ENISA)、由歐美亞太多家國際企業及標準

組織成立的非營利組織雲端安全聯盟(Cloud Security Alliance, CSA)……等，許多國際組織也有提出相關報告或見解。

2.4.2雲端服務高等級風險

而本研究強調要針對「雲端的高等級風險」因此要特別探討。首先是雲端安全聯盟(CSA)以「雲端運算關鍵區域安全指導綱要(Security Guidance for Critical Areas in Cloud Computing)」為基礎，所提出的七項「雲端建置需要考慮的首要威脅(Top Threats To Cloud Computing)」(CSA, 2010)：

一.濫用與惡意使用雲端服務：IaaS和PaaS服務商提供使用者資源無限的假象，而且要取得使用帳號非常容易，甚至有些服務商讓使用者連身份資料都不必留就可以免費使用服務。這使令資源可能被濫用，甚至是被用來為暴力破解程式、或殭屍網路提供強大運算資源。

二.安全的使用介面與API：雲端通常都透過網際網路提供服務，所以透過API和使用介面就能控制實際資源，而不需物理接觸。因此使用介面與API的安全就變得比過去更重要了。

三.惡意的內部員工：縱使所有駭客都難以入侵的資訊系統，如果碰到內部員工監守自盜同樣沒轍。更糟糕的是惡意員工平常就看起來和一般員工沒兩樣。

四.虛擬化技術問題：為了彈性應用資源、方便管理，IaaS服務商通常會使用虛擬化技術。而在同一台機器上的資源可以分租給不同使用者，但畢竟是住在同一棟樓，有心人仍有可能騷擾隔壁鄰居，稱做多租貸(multi-tenant)問題。

五.資料遺失或外洩：因為雲端上的交易(讀寫)次數增加，當然也增加資料可能會錯誤的風險，資料放在雲端上有可能會變得更危險。

六.帳號或服務被駭：帳號或服務被駭並不是個新風險，密碼通常會被重複使用，而且只需要帳號和密碼就可以在遠端取得完全控制。以網路為基礎的模式也不安全，駭客可能在服務商與客戶端間攔截封包，再回傳假訊息讓系統不知道已經被竊聽或控制。

七.未知風險輪廓：雲端其中一個好處是可以減少軟硬體擁有權，並專心於核心業務，但也可能過於專注核心業務而忽略資訊安全管理。軟體版本、程式碼更新、資安政策實行、系統弱點輪廓、入侵嘗試、資安機制設計、誰在分享你的資訊、網路入侵紀錄……等，所有細節都

是很重要的。也許你的系統正在被駭害而不自知。

另外開放網頁應用程式安全組織(Open Web Application Project,OWASP)在 2012 年提出的雲端十大安全風險(Cloud Top 10 Security Risks)則是較新的雲端風險因子辨識文件。OWASP 每年都在全球各地舉辦應用程式安全研討會(AppSec Conference)並發表許多重要資訊安全趨勢，是資訊開發人員在資訊安全方面重要的參考。OWASP 的雲端十大安全風險分別是以下十項：

T1.責任與資料擁有權(Accountability and Data Ownership)
T2.使用者身份識別的整合(User Identity Federation)
T3.法規適用性(Regulatory Compliance)
T4.業務持續運作與彈性(Business Continuity and Resiliency)
T5.用戶隱私與資料再利用(User Privacy and Secondary Usage of Data)
T6.服務與資料整合(Service and Data Integration)
T7.多租賃與實體資源安全(Multi Tenancy and Physical Security)
T8.事件分析與鑑識(Incidence Analysis and Forensic Support)
T9.基礎設施安全(Infrastructure Security)
T10.非開發環境揭露(Non Production Environment Exposure)

同樣有將雲端服務風險分級，但完整度及詳細度更高的是歐盟資訊安全組織ENISA提出的雲端服務風險評估報告(Cloud Computing Security Risk Assessment, CCSRA)，連CSA的雲端服務風險指導綱要也有引用這份報告。

ENISA提出的雲端服務風險評估報告(Cloud Computing Security Risk Assessment, CCSRA)參考了IDC、PCI DSS、NIST、ISO/IEC27001、ISA……等組織提出之報告標準及專家學者意見，整理出35項風險(包含政策與組織風險、技術風險、法律風險、非針對雲端的風險)、53項弱點(Vulnerabilities)、23項可能受影響資產(Assest)，又以其中九項風險被評為高風險(High)等級(ENISA, 2009)：

九項高等級風險如下：

一.R1.套牢(Lock-in)：只支援很少的工具、程序、資料格式及服務介面來保證資料、應用程式或服務的可攜性。這會讓客戶很難把資料或服務從某一雲端服務商遷移到另一個服務商或者是遷回公司內部環境。這使得服務從屬於某一特定雲端服務商，尤其是資料可攜性不被當成

基本原則時。

二.R2.失去對資料和系統控制權(Loss of Governance)：在使用雲端架構時，客戶一定要割讓控制權給雲端服務提供商，一定數量的雲端服務服務商會負擔安全議題。同時一部份的雲端服務商可能不會在服務水準協議(SLAs)中提供如此服務，因此在安全防禦間留下一個落差。

三.R3.承諾風險(COMPLIANCE RISKS)：如果雲端提供者不能提供他們自己承認的證據，或是不允許顧客對他們做稽核。這可能暗示有些承諾在公開雲架構無法被達成，當顧客遷移到雲上時會造成導致風險。

四.R9.隔離失效(ISOLATION FAILURE)：這是虛擬化技術導入後所產生的問題，雖然並非每片雲都有使用到虛擬化技術，但雲端和虛擬化技術卻常常伴隨著一起出現。多重租貸(multi-tenancy)與分享資源(shared resources)被定義為雲端運算的特性之一。這個風險種類包含在不同承租者間儲存體、記憶體路由器、甚至商譽隔絕的失敗 (例如：承租者 A 透過同伺服器上的承租者 B 當作跳板進行攻擊)。 然而也有人認為在這樣的隔絕機制下，攻擊者會較在傳統作業系統上進行攻擊更難。

五.R10.惡意的內部員工(MALICIOUS INSIDER) ：雖然通常比較少見，但內部員工有可能造成大深遠的傷害。雲端架構必須要依靠一些可靠的角色，這些人具有非常高的風險。例如說雲端提供商的管理員、及安全服務提供者。

六.R21.做為證物或電子蒐證(SUBPOENA AND E-DISCOVERY)：在法院強制執行或者公民提起訴訟的事件中查封實體硬體。資料集中儲存在資料中心並共用實體硬體意味著會有更多客戶暴露他們的資料在這項風險下。

七.R22.行政區的風險(RISK FROM CHANGES OF JURISDICTION)：客戶資料可能被儲存在多個行政區域，其中一些可能具有高風險。如果資料中心是在高風險國家(例如：某些缺乏法律規則、且有未知法律觀點和執行的國家，有獨裁警察的國家不會尊重國際協議，網站可能被當地政府授權突襲，資料和系統會被迫暴露或充公)。

八.R23.資料保護處理風險(DATA PROTECTION)：雲端運算造成好幾項資料保護風險。在一些狀況下，雲端客戶(身為資料控制者)可能很難有

效確認雲端提供者的資料處理實際狀況，也很難確認這些資料是否被合法處理。這個問題在多重資料傳輸(multiple transfers)狀況下被加重，例如：聯盟雲(federated clouds)。另一方面，有些雲端提供商確實提供他們所承載資料處理過程的資訊，有些也提供他們資料處理、安全活動和資料控制的認證。例如：SAS70 認證。

九.R.26 網路管理風險(NETWORK MANAGEMENT)：瀏覽器問題、網路壅塞、連接錯誤、非最佳化使用

與此九項風險相關之安全弱點(29 項)：

一.V1.粗略的授權認證與計費系統(AAA vulnerabilities)

一個粗劣的授權與計費系統可能會讓未授權的資源存取便容易，資源濫用與安全事件將會變得很普遍。除此之外，自從公司應用程式暴露在網際網路上開始，雲端模式就會讓針對密碼認證系統的攻擊(例如利用木馬程式竊取公司密碼)變得更有衝擊性。

二.V5.虛擬化弱點(Hypervisor vulnerabilities)：虛擬化層級的攻擊非常具有吸引力。虛擬機器事實上可以完全控制實體資源，所以這個層級的弱點相當關鍵。虛擬機器可能反客為主(guest to host escape)控制實體機器。另一個狀況是駭客可能從一個虛擬機器跳躍控制(VM hopping)另外一個虛擬機器。

三.V6.使用者間缺乏實體資源的獨立(Lack of resource isolation)
四.V7.使用者間缺乏商譽的獨立(Lack of reputational isolation)：一個客戶的活動，有可能影響到其他客戶的商譽。

五.V10.不能在加密狀態下處理資料(Impossibility of processing data in encrypted form)
六.V13.缺乏技術標準與標準解決方案(Lack of standard technologies and solutions)：意味著使用者可能會被套牢，也無法使用外部資訊安全管理工具。

七.V14.沒有原始碼託管協議(No source escrow agreement)：企業把開發系統的工作外包時,如果發現錯誤需要自行改寫時必須取得合法授權。缺乏這份原始碼託管協議，意味著如果 PaaS 或 SaaS 服務商破產時，顧客將無法自行修改系統。

八.V16.沒有控制漏洞評估程序(No control on vulnerability assessment process)：意味著把基礎架構弄安全的責任就交到客戶手上了。

九.V17.可能在內部或雲端網路上發生的掃瞄(Possibility that internal/cloud network probing will occur)：一個使用者可能會在另外一個使用者的內部網路或雲端網路做漏洞掃描。

十.V18.使用者可能會對鄰居的資源做偵測(Possibility that co-residence checks will be performed)
十一.V21.合約沒有寫清楚責任歸屬(Synchronizing responsibilities or contractual obligations external to cloud)：許多使用者沒有察覺到服務中的某些責任屬於自己，甚至像是加密檔案，這些都是要在合約中講清楚的。

十二.V22.跨雲端應用程式隱含相依關係(Cross-cloud applications creating hidden dependency)：服務供應鏈中存在隱藏的相依關係(雲內和外的相依),當第三方開發商(轉包商或客戶的公司)擴充服務系統時，IaaS 或 PaaS 雲端服務商的架構不支援。

十三.V23.服務水平協議條款可能會在不同利害關係人間產生互斥(SLA clauses with conflicting promises to different stakeholders)：服務水平協議(SLA)條款可能也會和其他服務商承諾或條款產生互斥。

十四.V25.雲端服務商無法藉由稽核或認證給予客戶任何保證(Audit or certification not available to customers)
十五.V26.認證計畫不適合雲端架構(Certification schemes not adapted to cloud infrastructures)
十六.V29.資料被儲存在多個司法行政區，但在這件事上缺乏透明度(Storage of data in multiple jurisdictions and lack of transparency about THIS)
十七.V30.缺少該資料儲存所在司法行政區的相關資訊(Lack of information on jurisdictions)
十八.V31.使用者條款缺乏完整性與透明度(Lack of completeness and transparency in terms of use)
十九.V34.雲端服務提供商組織裡的角色與責任定義不明確(Unclear roles and responsibilities)
二十.V35.雲端服務提供組織裡角色職責實行不確實 (Poor enforcement of role definitions)：可能創造某一個權力過大的管理角色。

二十一.V36.相關當事人知道太多非必要的細節(Need-to-know principle

not applied)：相關當事人只需要知道原則而不是太多非必要細節。

二十二.V37.不充分的技術實體安全(Inadequate physical security procedures)：例如 RFID 的資安問題、或沒有電磁保護避免竊聽

二十三.V38.人為設定錯誤(Misconfiguration)：不適當的應用程式安全設定、僵化程序、人為失誤、未受訓練的管理員。

二十四.V39.系統或作業系統弱點(System or OS vulnerabilities)
二十五.V41.缺乏或很差的持續營運與災難復原計畫(Lack of, or a poor and untested, business continuity and disaster recovery PLAN)
二十六.V44.資產擁有權不明確(Unclear asset ownership)
二十七.V46.太少雲端服務商可以供選擇(Poor provider selection)
二十八.V47.缺乏生產者剩餘(Lack of supplier redundancy)：意味著服務商沒有超額利潤

二十九.V48.應用程式弱點或粗劣的更新檔管理(Application vulnerabilities or poor patch management)

受此九項風險影響之資產(12 項)：

一.A1.使用者的商譽(Company reputation)
二.A2.使用者的顧客信賴(Customer trust)：包含友好度，可以從客訴衡量
三.A3.使用者的員工忠誠與經驗(Employee loyalty and experience)
四.A4.使用者的智慧財產(Intellectual property)
五.A5.敏感的個人資料(Personal sensitive data)：意指會令人種或人種來源、宗教哲學或其他信仰、政治傾向、社群成員、商業聯盟、宗教或政治組織.....等，敏感資料曝光的個人資料。

六.A6.使用者及服務商的個人資料(Personal data)：「係指任何可以辨識資料出資料擁有者本人(自然人)是誰的資訊。可以辨識的人指的是某人在特殊狀況下可以被間接或直接認出來，舉凡身分證號碼、身體、生理、心裡、經濟、文化、或社會身份……等，都是個人資料。(European Parliament, 1995)」

七.A7.使用者及服務商的關鍵個人資料(Personal data – critical)：組織認為非常重要的資料

八.A8.日常資料(HR data)：營運相關但被排除在資料保護範圍外的資料。

九.A9.需要即時提供的服務(Service delivery – real time services)

十.A10.服務提供(Service delivery)
十一.A16.網路(Network)：包含雲內互聯或雲內外的連接
十二.A20.認證(Certification)：ISO、PCI DSS……等等。

至於各個弱點、風險、資產對應關係見表 2-2：

表 2-2-1.雲端運算高等級風險、弱點、與資產

弱點	風險	資產
・政策與組織風險		
V13,V31,V46,V47	R1.套牢(Lock-in)	A1,A5,A6,A7, A9,A10
V13,V14,V16,V21, V22,V23,V25,V26, V29,V30,V31,V34, V35,V44	R2.失去對資料和系統控制權(Loss of Governance)	A1,A2,A3,A5, A6,A7,A9,A10
V13,V25,V26, V29,V30,V31	R3. 承諾風險(COMPLIANCE RISKS)	A20
・技術風險		
V5,V6,V7, V17,V18	R9. 隔離失效(ISOLATION FAILURE)	A1,A2,A5,A6, A7,A9,A10
V1,V10,V34,V35, V36,V37,V39,V48	R10.惡意的內部員工(MALICIOUS INSIDER)	A1,A2,A3,A4,A5, A6,A7,A8,A9,A10
V6,V38,V39,V41	R26.網路管理風險(NETWORK MANAGEMENT)	A1,A2,A3, A9,A10,A16

資料來源：ENISA(2009), ‘Cloud Computing Security Risk Assessment’, European Network and Information Security Agency

表 2-2-2.雲端運算高等級風險、弱點、與資產

・法律風險		
V6,V29,V30	R21.作為證物或電子蒐證 (SUBPOENA AND E-DISCOVERY)	A1,A2,A5,A6, A7,A9,A10
V29,V30	R22.行政區的風險 (RISK FROM CHANGES OF JURISDICTION)	A1,A2,A5,A6, A7,A9,A10
V29,V30	R23.資料保護處理風險 (DATA PROTECTION)	A1,A2,A5,A6, A7,A9,A10

資料來源：ENISA(2009), 'Cloud Computing Security Risk Assessment', European Network and Information Security Agency

第三章、研究方法

本章依序探討本研究之研究流程、限制假設、測量方法、及分析方法。

3.1 研究流程

如圖 3-1 所示，根據 2.2 節提到風險管理步驟來看。第一階段風險辨識(重要風險、弱點、受影響資產)因為因子定義最清楚且全面的關係，選用 ENISA 提出的雲端服務風險評估報告(Cloud Computing Security Risk Assessment, CCSRA)，同時 ENISA 身為歐盟標準組織具有公信力。本研究要進行的步驟是第二階段風險衡量，建立風險衡量模式的演算法來自文獻，資料由問卷取得，半數資料推測模式參數，另一半做比較。然後分析弱點、風險、受影響資產間的關係供往後決策者或研究人員作決策參考。

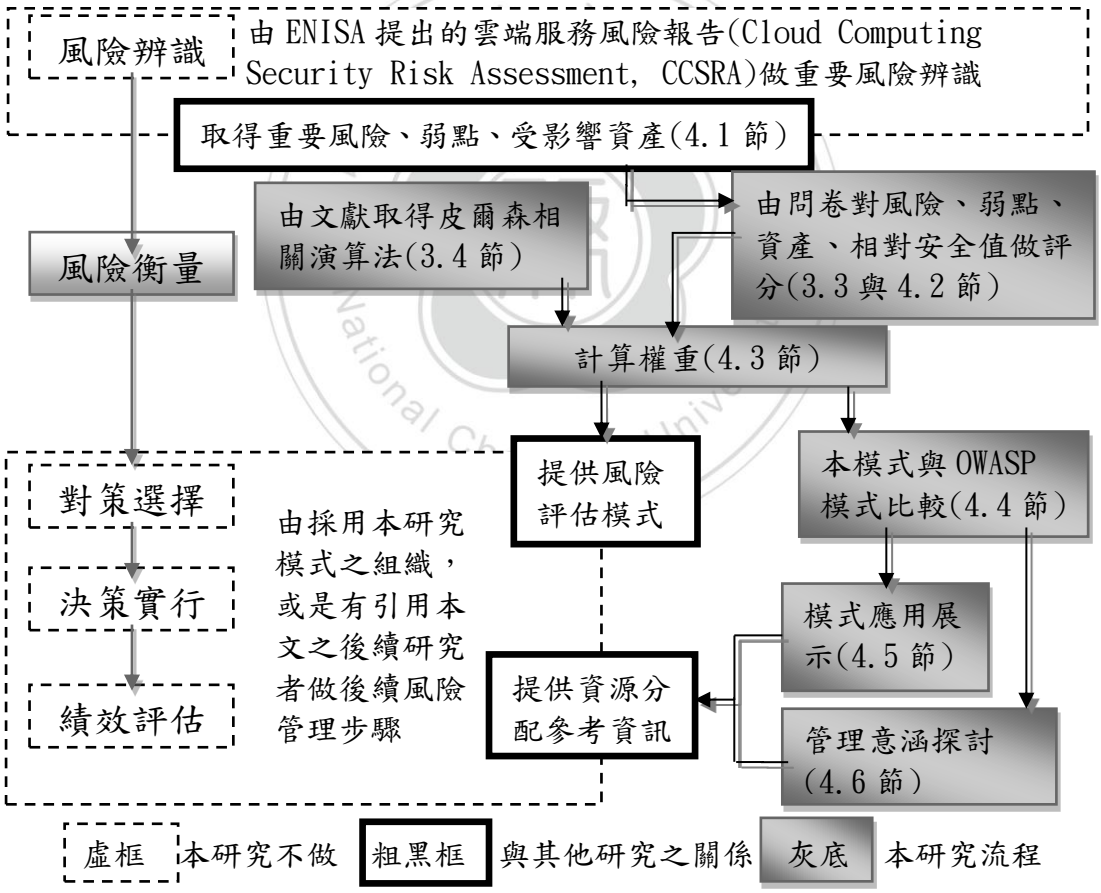


圖 3-1. 研究流程
本研究繪製

3.2 研究限制及預設推論

資訊安全議題發展至今，各種風險問題隨著技術發展、服務模式改變而有增無減，更遑論屬於技術匯流又具有多種服務模式的雲端運算了。因此要完整評估一個雲端運算風險模式問項題數可能會高達100~200 多題，考慮到問卷回收率及成本問題，因此僅做高等級的雲端服務風險，但何謂「高等級」風險？因為報告分析完整度考量及組織公信力，以 ENISA 提出的雲端服務風險評估報告(Cloud Computing Security Risk Assessment, CCSRA)中相關專家評估為高等級(High)的風險，也因為模式精細度需求將原本五分等級評分增加一倍(變成十等級)。

另外必須預設以下幾點推論(圖 3-2)：

推論 1：有弱點(vulnerability)暴露才會造成風險(Risk)，因此評估可能導致此風險的弱點，就可以推算出此風險發生率。

推論 2：風險(Risk)需要對資產(Assets)造成傷害才可能有損失(Loss)發生，因此評估該風險影響資產的程度、及該資產重要性可推估出該風險事件嚴重程度。

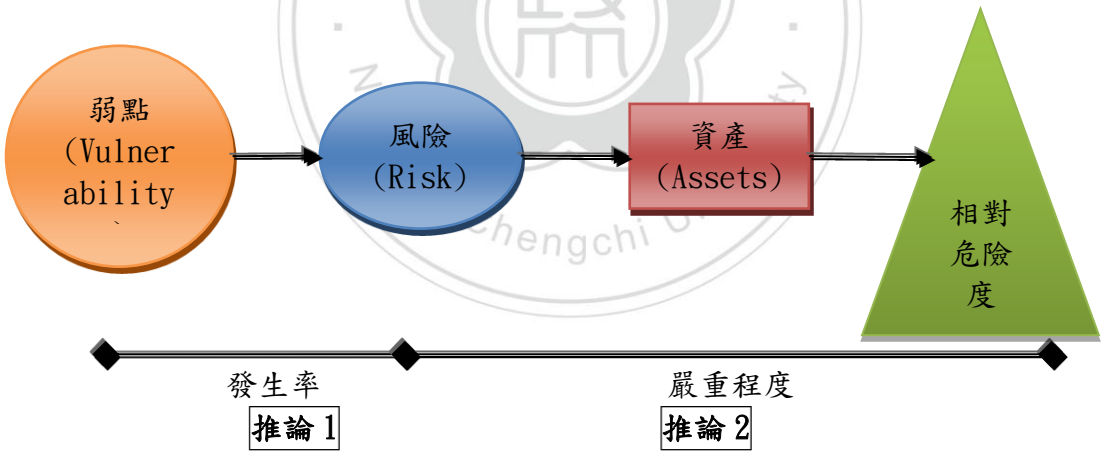


圖 3-2. 弱點、風險、資產之因果關係
本研究繪製

3.3 研究問卷設計

本研究使用問卷調查法取得雲端服務風險實際運作狀況，並推算出最佳模式參數。因此本研究問卷將請問卷對象針對風險(Risk)、弱點(vulnerability)評估符合程度、及針對資產(Assest)評估危險程度、還要評估一個相對危險值。

在問卷對象方面，將針對在乎雲端服務風險、且對相關技術風險

有所了解、並長期關注雲端服務的相關人員。因此排除一般消費大眾，針對台灣雲端運算協會的會員做發放，填答者必須是有在負責(或使用)雲端業務的人。同時為了避免填答者誤會各項目意義，會以找到的風險名稱再多做簡短、清楚的解釋。這裡要特別說明的是風險與弱點的符合程度越高代表該風險發生率越高，而資產安全度與相對危險度越高代表越安全。表 3-1 是本研究之問卷範例示意：

表 3-1-1. 研究問卷範例示意

雲端服務高等級風險評估調查

您好，我是政大資管研究生羅邵晏。以下是本問卷基本介紹：

・研究主題：「皮爾森相關係數法建立雲端服務高等級風險之評估模式」

・問卷對象：組織中在乎雲端服務風險、長期接觸相關業務、並對相關技術及合約條款知悉之人員

・尋求資訊：[Part1] XX 項風險符合程度、

[Part2] XX 項資產危險程度、

[Part3] XX 項弱點符合程度、

[Part4] 整體使用的危險程度評分及基本資料

・作答時間：約 XX 分鐘

政大資管 羅邵晏 研究生

指導教授 林我聰 博 士

感謝您的配合

Part1:請依據**您使用雲端服務狀況**，為以下 9 項風險評分											
風險名稱	**符合程度(單選題，請打勾)**										
	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100
(1)被雲端服務商套牢(更換服務商困難)											
…											
(9)網路管理風險											

Part2:**請依據**您使用雲端服務狀況，**為以下 12 項資產評分**											
資產名稱	**危險程度(單選題，請打勾)**										
	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100
(1)											
……											
(12)											

本研究設計

表 3-1-2. 研究問卷範例示意

Part3:**請依據**您使用雲端服務狀況，**為以下 29 項弱點評分**											
弱點名稱	**符合**程度(**單選題，請打勾**)										
	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100
(1)											
…											
(29)											

Part4:基本資料(**個別資料只做研究應用，絕不對外公開**)
(1)請問貴公司使用(或提供)的雲端**服務類型**(可複選)：□SaaS □PaaS □LaaS
(2)請問貴公司使用(或提供)的**雲種類**：□公有雲 □私有雲 □混合雲 □其他_____
(3)請問貴公司使用(或提供)雲服務的**時間**：□不到 1 年 □2~3 年 □3~4 年 □____年
(4)請給貴公司使用(或提供)的雲端服務**危險程度**評分**(0~100)**：_____
(5)請問貴公司使用的**雲端服務廠商**是(雲端**服務提供商**請填寫**提供的服務內容**)：_____

本研究設計

3.4 風險評估模式建立方法

模式建立可以分成以下步驟：

1. 找弱點、風險、資產
2. 計算弱點、風險、資產、相對危險度間的權重關係

除第一步驟以文獻探討處理外，本節主要討論第二步驟找權重的方法。在各領域都有各自的量化風險評估模式，工業安全方面有道氏指數(Dow Index) & 邦德指數(Mond Index)、失誤樹分析(FTA) & 事件樹(ETA)。在財務會計領域有區別分析(DA)、邏輯斯迴歸(logistic regression)、Probit、類神經網路(ANN)、支持向量機(SVM)。同時皮爾森相關係數法(Pearson Correlation)也常被用來分析兩因子間相關程度，在使用上非常方便。只要一個數值變成判斷兩因子間正向或負向相關程度，但只能用於線性相關。(表 3-2)

表 3-2.量化風險評估模式比較		
方法	優點	缺點
類神經網路(Neural Network)	不假設樣本為常態分配，也無共線性問題	模式計算是黑箱作業，無法看出變數間關係
邏輯斯迴歸(logistic regression)	適用於非線性性狀況	因變數只能是 0 或 1
失誤樹分析(FTA) & 事件樹(ETA)	易知事件時間順序間邏輯關係、定性又定量、邏輯簡單易懂、定性又定量	可能忽略一些事件、分析者需要具備分析技術、故障率不易取得、可能不是深度且詳細分析
路徑分析(Path Analysis)	對研究變數間因果關係是個很方便的工具	模型建構錯誤會讓模式失準、不重視對誤差處理、著重於整體模式對於個別變數的解釋較弱
皮爾森相關(Pearson Correlation)	使用上方便、簡單易懂、能看出個別變項的正向或負向關係	只能用於線性相關

資料來源：本研究整理

為了能配合弱點、風險、資產的三層結構，觀察它們之間相互影響的關係，且兼顧對各別變數的解釋。因此本研究使用皮爾森相關方法推算各因子間的影響係數做為權重。

3.4.1 皮爾森相關

賴世培&詹志禹(2001)提到「我們利用雙變數資料，便可以研究互相關聯的問題。當一個變項變大時，另一個變項亦隨之有系統的變大稱之為正相關。當一個變項變大時，另一個變項亦隨之有系統的變小稱之為負相關。兩變項之間相互發生的關聯可經由資料散布圖或經由計算相關係數來得知，此相關是否為正或負，及其相關程度的強弱又是如何。相關的技術在社會科學上的應用是非常之廣。……而皮爾森相關(Pearson Correlation)是最常用的相關技術，是由英國統計學家皮爾森(Karl Pearson)所提出…」

Egghe & Leydesdorff(2009)則對皮爾森相關的優缺點有所評論「一般來說，皮爾森相關只能用來衡量線性相關的程度...而皮爾森相關值很方便，因為只需要一個數字便能區分出正相關與負相關程度。」

而Iuga(2010)指出皮爾森相關係數是一個無維度(dimensionless)的

指標，值域在-1~1之間，並能反映兩組資料間的線性關係。而計算如式1，把x和y兩因子的共變異數除上兩者標準差之積，或是把xy積之算術平均減去x和y各自算術平均之積，然後再除上x和y的標準差：

$$R = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{M(xy) - M(x)M(y)}{\sigma_x \sigma_y} \in [-1,1] \quad (1)$$

R:皮爾森相關係數

Cov(x,y)：x和y的共變異數

σ_a：a的標準差

M(a)：a的算術平均值

計算結果 R>0 代表 x 增加 y 也會一起增加，而 R<0 代表 x 增加 y 反而會變小，R=0 代表兩者無相關性。

3.4.2 研究模式示意圖

如圖 3-3 所示，從文獻中找出各弱點、風險、資產對應關係，再由本研究設計之問卷將各對應關係線上的權重計算出來：

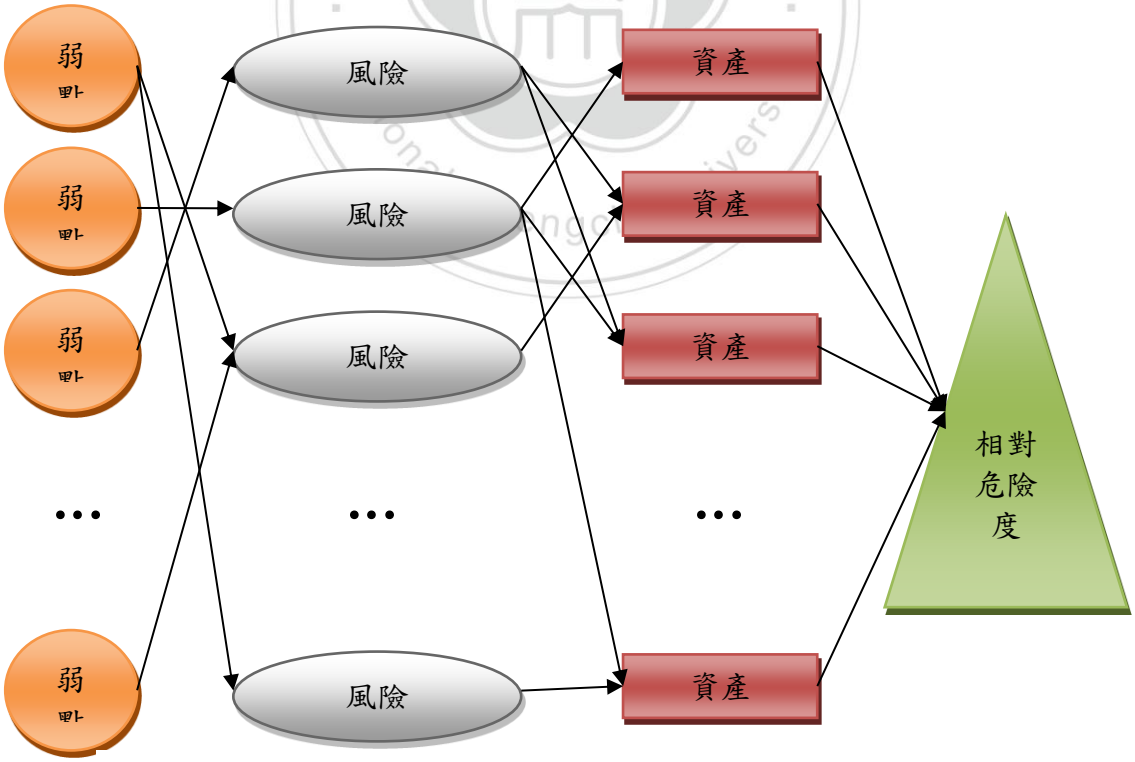


圖 3-3. 弱點、風險、資產、相對危險度因果關係示意

本研究繪製

第四章、風險評估模式建立、對照與使用

4.1 尋找弱點、風險、資產

本節主要工作是要找出有哪些高等級弱點、風險、資產與他們間的對應關係(參考圖 3-1 研究流程)。見圖 4-1，本研究以 ENISA 提出的雲端服務風險評估報告(Cloud Computing Security Risk Assessment, CCSRA)中相關專家評估為高等級(High)的風險以及對應弱點和資產作為模式建立之用(原本報告中有 53 項弱點、35 項風險、23 項資產，屬於高等級風險有 9 項，此 9 風險對應 29 項弱點及 12 項資產)

R.1 LOCK-IN

Probability	HIGH	Comparative: Higher
Impact	MEDIUM	Comparative: Equal
Vulnerabilities	V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

圖 4-1.ENISA 報告中第一個高等級風險

資料來源：ENISA(2009), 'Cloud Computing Security Risk Assessment', European Network and Information Security Agency

經過萃取後詳細內容，資產對應相對危險度(表 4-1)、弱點對風險(表 4-2)、風險對資產(表 4-3)分別如下：

表 4-1-1.資產對相對危險度的皮爾森相關式

資產			
A1	使用者的商譽(Company reputation)	→	相對危險度
A2	使用者的顧客信賴(Customer trust)	→	
A3	使用者的員工忠誠與經驗(Employee loyalty and experience)	→	

本研究繪製

表 4-1-2.資產對相對危險度的皮爾森相關式

A4	使用者的智慧財產(Intellectual property)	→	相對危險度
A5	敏感的個人資料(Personal sensitive data)	→	
A6	使用者及服務商的個人資料(Personal data)	→	
A7	使用者及服務商的關鍵個人資料(Personal data – critical)	→	
A8	日常資料(HR data)	→	
A9	需要即時提供的服務(Service delivery – real time services)	→	
A10	服務提供(Service delivery)	→	
A16	網路(Network)	→	
A20	認證(Certification)	→	

本研究繪製

表 4-2-1. 弱點對風險的皮爾森相關式

弱點	風險
V13 缺乏技術標準與標準解決方案	R1 套牢
V31 使用者條款缺乏完整性與透明度	
V46 太少雲端服務商可以供選擇	
V47 缺乏生產者剩餘	
V13 缺乏技術標準與標準解決方案	R2 失去對資料和系統控制權
V14 沒有原始碼託管協議	
V16 沒有控制漏洞評估程序	
V21 合約沒有寫清楚責任歸屬	
V22 跨雲端應用程式隱含相依關係	
V23 服務水平協議條款可能會在不同利害關係人間產生互斥	
V25 雲端服務商無法藉由稽核或認證給予客戶任何保證	
V26 認證計畫不適合雲端架構	
V29 資料被儲存在多個司法行政區，但在這件事上缺乏透明度	
V30 缺少該資料儲存所在司法行政區的相關資訊	
V31 使用者條款缺乏完整性與透明度	
V34 雲端服務提供商組織裡的角色與責任定義不明確	
V35 雲端服務提供組織裡角色職責實行不確實	
V44 資產擁有權不明確	

資料來源：ENISA(2009), ‘Cloud Computing Security Risk Assessment’, European Network and Information Security Agency

表 4-2-2 弱點對風險的皮爾森相關式

V13	缺乏技術標準與標準解決方案	R3 承諾風險
V25	雲端服務商無法藉由稽核或認證給予客戶任何保證	
V26	認證計畫不適合雲端架構	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	
V30	缺少該資料儲存所在司法行政區的相關資訊	
V31	使用者條款缺乏完整性與透明度	
V5	虛擬化弱點	R9 隔離失效
V6	使用者間缺乏實體資源的獨立	
V7	使用者間缺乏商譽的獨立	
V17	可能在內部或雲端網路上發生的掃瞄	
V18	使用者可能會對鄰居的資源做偵測	
V1	粗略的授權認證與計費系統	R10 惡意的內部員工
V10	不能在加密狀態下處理資料	
V34	雲端服務提供商組織裡的角色與責任定義不明確	
V35	雲端服務提供組織裡角色職責實行不確實	
V36	相關當事人知道太多非必要的細節	
V37	不充分的技術實體安全	
V39	系統或作業系統弱點	
V48	應用程式弱點或粗劣的更新檔管理	
V6	使用者間缺乏實體資源的獨立	R26 網路管理風險
V38	人為設定錯誤	
V39	系統或作業系統弱點	
V41	缺乏或很差的持續營運與災難復原計畫	
V6	使用者間缺乏實體資源的獨立	R21 作為證物或電子蒐證
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	
V30	缺少該資料儲存所在司法行政區的相關資訊	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	R22 行政區的風險
V30	缺少該資料儲存所在司法行政區的相關資訊	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	R23 資料保護處理風險

資料來源：ENISA(2009), ‘Cloud Computing Security Risk Assessment’, European Network and Information Security Agency

表 4-3-1. 風險對資產的皮爾森相關式

風險	資產
R10 惡意的內部員工	A1 使用者的商譽
R1 套牢	
R2 失去對資料和系統控制權	
R9 隔離失效	
R26 網路管理風險	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	
R1 套牢	A10 服務提供
R2 失去對資料和系統控制權	
R9 隔離失效	
R10 惡意的內部員工	
R26 網路管理風險	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	
R26 網路管理風險	A16 網路
R10 惡意的內部員工	A2 使用者的顧客信賴
R2 失去對資料和系統控制權	
R9 隔離失效	
R26 網路管理風險	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	
R3 承諾風險	A20 認證
R2 失去對資料和系統控制權	A3 使用者的員工忠誠與經驗
R10 惡意的內部員工	
R26 網路管理風險	
R10 惡意的內部員工	A4 使用者的智慧財產

資料來源：ENISA(2009), 'Cloud Computing Security Risk Assessment', European Network and Information Security Agency

表 4-3-2. 風險對資產的皮爾森相關式

R1 套牢	A5 敏感的個人資料
R2 失去對資料和系統控制權	
R9 隔離失效	
R10 惡意的內部員工	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	
R1 套牢	A6 使用者及服務商的個人資料
R2 失去對資料和系統控制權	
R9 隔離失效	
R10 惡意的內部員工	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	
R1 套牢	A7 使用者及服務商的關鍵個人資料
R2 失去對資料和系統控制權	
R9 隔離失效	
R10 惡意的內部員工	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	
R10 惡意的內部員工	A8 日常資料
R1 套牢	A9 需要即時提供的服務
R2 失去對資料和系統控制權	
R9 隔離失效	
R10 惡意的內部員工	
R26 網路管理風險	
R21 作為證物或電子蒐證	
R22 行政區的風險	
R23 資料保護處理風險	

資料來源：ENISA(2009), ‘Cloud Computing Security Risk Assessment’, European Network and Information Security Agency

4.2 基本資料分析

對應 3-3 節所設計之問卷，本研究以郵寄方式共發送問卷 111 份，回收 12 份，其中 11 份有效問卷，填答者以主管策略人員及專案經理為主，平均使用或提供雲端服務 2.2 年。其中使用雲種類及雲服務類型如表 4-4 所示：

表 4-4. 問卷對象提供或使用之雲服務分佈

SaaS	4/11	1/11	4/11
PaaS	3/11	1/11	3/11
IaaS	7/11	1/11	2/11
雲服務 / 雲種類	私有雲	混和雲	公有雲

說明：一家廠商可能有多種服務(例如：私有雲 4+3+7=14>11 代表至少有 3 家廠商同時提供兩種以上服務)，一家廠商也不一定會使用或提供所有服務(例如：SaaS 4+1+4=9<11 代表有 2 家廠商未提供 SaaS 服務)

本研究繪製

從上表中可以看出目前企業仍然對公有雲具有一定的不信任程度，因此私有雲仍然是最受歡迎的選項。

4.3 模式建立

經過 3-4-1 節介紹的皮爾森相關係數計算後算出各個對應弱點、風險、資產、和總分間的權重分別如表 4-5、表 4-6、表 4-7，其中係數大於零代表正向關係，小於零則是負向關係：

表 4-5-1.弱點對風險的皮爾森相關係數

弱點	係數	風險
V13 缺乏技術標準與標準解決方案	0.643308	R1 套牢
V31 使用者條款缺乏完整性與透明度	0.152965	
V46 太少雲端服務商可以供選擇	0.121682	
V47 缺乏生產者剩餘	-0.31388	

本研究繪製

表 4-5-2.弱點對風險的皮爾森相關係數

V13	缺乏技術標準與標準解決方案	0.301515	R2 失去對資料和系統控制權
V14	沒有原始碼託管協議	0.587683	
V16	沒有控制漏洞評估程序	0.538764	
V21	合約沒有寫清楚責任歸屬	0.255858	
V22	跨雲端應用程式隱含相依關係	-0.12849	
V23	服務水平協議條款可能會在不同利害關係人間產生互斥	0.142596	
V25	雲端服務商無法藉由稽核或認證給予客戶任何保證	0.218795	
V26	認證計畫不適合雲端架構	-0.03052	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	0.536722	
V30	缺少該資料儲存所在司法行政區的相關資訊	0.304881	
V31	使用者條款缺乏完整性與透明度	0.517488	
V34	雲端服務提供商組織裡的角色與責任定義不明確	0.304161	
V35	雲端服務提供組織裡角色職責實行不確實	0.557318	
V44	資產擁有權不明確	0.433519	
V13	缺乏技術標準與標準解決方案	-0.17564	R3 承諾風險
V25	雲端服務商無法藉由稽核或認證給予客戶任何保證	-0.36637	
V26	認證計畫不適合雲端架構	0.019895	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	0.35926	
V30	缺少該資料儲存所在司法行政區的相關資訊	0.151065	
V31	使用者條款缺乏完整性與透明度	0.48967	
V5	虛擬化弱點	0.588155	R9 隔離失效
V6	使用者間缺乏實體資源的獨立	0.478238	
V7	使用者間缺乏商譽的獨立	0.39211	
V17	可能在內部或雲端網路上發生的掃瞄	0.451577	
V18	使用者可能會對鄰居的資源做偵測	0.481582	

本研究繪製

表 4-5-3.弱點對風險的皮爾森相關係數

V1	粗略的授權認證與計費系統	0.757214	R10 惡意的內部員工
V10	不能在加密狀態下處理資料	0.375566	
V34	雲端服務提供商組織裡的角色與責任定義不明確	0.067981	
V35	雲端服務提供組織裡角色職責實行不確實	0.214882	
V36	相關當事人知道太多非必要的細節	0.168191	
V37	不充分的技術實體安全	0.317537	
V39	系統或作業系統弱點	0.36618	
V48	應用程式弱點或粗劣的更新檔管理	0.814367	
V6	使用者間缺乏實體資源的獨立	0.739145	R26 網路管理風險
V38	人為設定錯誤	0.413864	
V39	系統或作業系統弱點	0.344509	
V41	缺乏或很差的持續營運與災難復原計畫	0.378374	
V6	使用者間缺乏實體資源的獨立	0.378617	R21 作為證物或電子蒐證
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	-0.30274	
V30	缺少該資料儲存所在司法行政區的相關資訊	-0.38669	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	0.555071	R22 行政區的風險
V30	缺少該資料儲存所在司法行政區的相關資訊	0.479461	
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	-0.29632	R23 資料保護處理風險
V30	缺少該資料儲存所在司法行政區的相關資訊	0.209757	

本研究繪製

表 4-6-1.風險對資產的皮爾森相關係數

風險	係數	資產
R10 惡意的內部員工	0.500585	A1 使用者的商譽
R1 套牢	0.158755	
R2 失去對資料和系統控制權	0.445208	
R9 隔離失效	0.376986	
R26 網路管理風險	0.5418	
R21 作為證物或電子蒐證	0.160876	
R22 行政區的風險	0.675866	
R23 資料保護處理風險	0.424022	
R1 套牢	0.257163	A10 服務提供
R2 失去對資料和系統控制權	0.289274	
R9 隔離失效	0.400158	
R10 惡意的內部員工	0.414453	
R26 網路管理風險	0.575568	
R21 作為證物或電子蒐證	0.419217	
R22 行政區的風險	0.475465	
R23 資料保護處理風險	0.705319	
R26 網路管理風險	0.339754	A16 網路
R10 惡意的內部員工	0.594418	A2 使用者的顧客信賴
R2 失去對資料和系統控制權	0.486305	
R9 隔離失效	0.278904	
R26 網路管理風險	0.556504	
R21 作為證物或電子蒐證	0.10217	
R22 行政區的風險	0.703789	
R23 資料保護處理風險	0.395361	
R3 承諾風險	0.384183	A20 認證
R2 失去對資料和系統控制權	0.569781	A3 使用者的員工忠誠與經驗
R10 惡意的內部員工	0.70873	
R26 網路管理風險	0.702355	

本研究繪製

表 4-6-2.風險對資產的皮爾森相關係數

R10 惡意的內部員工	0.645739	A4 使用者的智慧財產
R1 套牢	0.625768	A5 敏感的個人資料
R2 失去對資料和系統控制權	0.340776	
R9 隔離失效	0.080147	
R10 惡意的內部員工	0.465456	
R21 作為證物或電子蒐證	0.67007	
R22 行政區的風險	0.594831	
R23 資料保護處理風險	0.234668	
R1 套牢	0.331336	A6 使用者及服務商的個人資料
R2 失去對資料和系統控制權	0.08977	
R9 隔離失效	0.04726	
R10 惡意的內部員工	0.254995	
R21 作為證物或電子蒐證	0.327086	
R22 行政區的風險	0.319142	
R23 資料保護處理風險	0	
R1 套牢	0.22897	A7 使用者及服務商的關鍵個人資料
R2 失去對資料和系統控制權	0.054632	
R9 隔離失效	0.041768	
R10 惡意的內部員工	0.26113	
R21 作為證物或電子蒐證	0.287678	
R22 行政區的風險	0.316384	
R23 資料保護處理風險	0.252886	
R10 惡意的內部員工	0.258715	A8 日常資料
R1 套牢	0.356348	A9 需要即時提供的服務
R2 失去對資料和系統控制權	0.126645	
R9 隔離失效	0.2159	
R10 惡意的內部員工	0.141404	
R26 網路管理風險	0.172241	
R21 作為證物或電子蒐證	0.123753	
R22 行政區的風險	0.302498	
R23 資料保護處理風險	0.181509	

本研究繪製

表 4-7.資產對總分的皮爾森係數

資產		係數	
A1	使用者的商譽(Company reputation)	0.777429	
A2	使用者的顧客信賴(Customer trust)	0.793538	
A3	使用者的員工忠誠與經驗(Employee loyalty and experience)	0.760062	
A4	使用者的智慧財產(Intellectual property)	0.736031	
A5	敏感的個人資料(Personal sensitive data)	0.937149	相對危險度
A6	使用者及服務商的個人資料(Personal data)	0.92192	
A7	使用者及服務商的關鍵個人資料(Personal data – critical)	0.890641	
A8	日常資料(HR data)	0.922844	
A9	需要即時提供的服務(Service delivery – real time services)	0.852595	
A10	服務提供(Service delivery)	0.792962	
A16	網路(Network)	0.91695	
A20	認證(Certification)	0.792962	

本研究繪製

其中要注意的是以下個對應關係係數呈現非預期結果(原本預期應該所有係數都大於零)，以及造成此結果的可能原因如下表 4-8：

表 4-8-1.非預期關係解釋

風險	係數	資產	可能原因
R23 資料保護處理風險	0	A6 使用者及服務商的個人資料	國內雲端服務起步較晚，有很多雲端服務商尚未取得安全認證。但使用者相信在個資法通過後，競爭激烈的台灣資訊產業仍然會促使服務商建立完善的個人資料保護機制。
弱點	係數	風險	可能原因
V47 缺乏生產者剩餘	-0.31388	R1 套牢	國內服務商多、殺價競爭，業者為了搶客願意承受與分攤使用者轉嫁的轉換成本。

本研究繪製

表 4-8-2.非預期關係解釋

V22 跨雲端應用程式隱含相依關係	-0.12849	R2 失去對資料和系統控制權	國內雲端服務發展較晚且較重視硬體能力，所以相對而言接受 IaaS 服務的使用者不認為 SaaS 層級應用程式間相依關係高是大問題。
V26 認證計畫不適合雲端架構	-0.03052		國內企業雲端服務仍以 IaaS 與私有雲為大宗，使用者仍然掌握大部分控制權。
V13 缺乏技術標準與標準解決方案	-0.17564	R3 承諾風險	國內軟體產業競爭激烈，服務商擔心失去客戶，沒有標準解決方案，反而會讓各服務商投入更多資源達成讓顧客放心的目標。
V25 雲端服務商無法藉由稽核或認證給予客戶任何保證	-0.36637		國內雲端服務以私有雲及 IaaS 為主，客戶仍然掌控大部份資料與系統。SaaS 客戶則因為國內軟體廠商眾多，相信服務商必定會為了留住客戶做好相關安全措施，所以並不必要對服務商做稽核。
V29 資料被儲存在多個司法行政區，但在這件事上缺乏透明度	-0.30274	R21 作為證物或電子蒐證	國內目前以 IaaS 及私有雲為主的雲端服務環境下，企業使用者可以掌握資料儲存區域，所以比較沒有因為不知道資料儲存在哪個國家，而擔心伺服器被法院扣押會資料外洩的疑慮。
V30 缺少該資料儲存所在司法行政區的相關資訊	-0.38669		在國內產業競爭環境下，雲端使用者相信服務商在部份實體資源被法院扣押時能確實啟用其他備份系統以防止客戶流失，而伺服器存放在執法機關反而更能保護與無關案件者的資料保密權益。
V29 資料被儲存在多個司法行政區，但在這件事上缺乏透明度	-0.29632	R23 資料保護處理風險	國內目前以 IaaS 和私有雲為主的雲端服務大部分系統和資料仍在使用者掌控下。SaaS 部分則可能是因為國內軟體業競爭度高，使用者相信就算沒有藉由認證證明，服務商仍然會令資料處理過程最安全且完全合法，作為留住客戶基本目標。

本研究繪製

4.4 本模式與 OWASP 模式比較

在上一節中我們利用弱點、風險、資產、和總分間的皮爾森相關係數建立量化模式，並針對非預期結果做出可能原因的解釋。在本節中將隨機產生 10 家服務商的弱點評分，利用本研究模式計算相對危險度並做服務商安全度排名。另外再根據文獻對雲端弱點的分類，計算出另外一種服務商相對危險度分數排名，並和本研究模式計算出的安全度排名做比較看看是否相符(圖 4-2)：

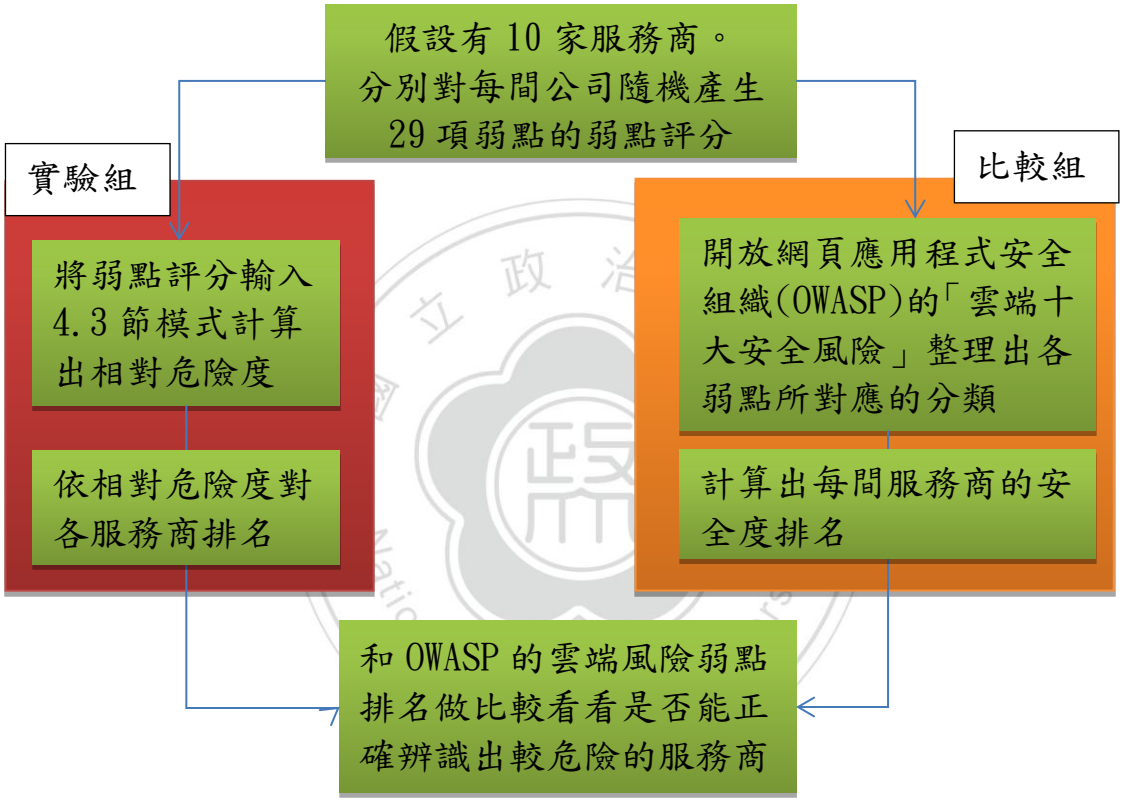


圖 4-2.本研究模式之比較流程
本研究設計

4.4.1 比較組廠商排名之計算

首先由開放網頁應用程式安全組織(Open Web Application Project,OWASP)提出的雲端十大安全風險(Cloud Top 10 Security Risks)對弱點進行分類。採用 OWASP 提出的報告是因為這是目前最新、且較具共識的雲端服務風險報告。

需要特別說明的一點是此 29 項弱點在 OWASP 十大安全風險報告中雖然全部都找到各自對應風險類別，但是「T2 使用者份識別整合」和「T10 非開發環境揭露」兩類風險並沒有被任何本研究使用之弱點歸

屬，因為本研究使用之 ENISA 報告站在使用者觀點，但 OWASP 報告是站在 SaaS 雲端應用程式開發者的角度。(表 4-9)

表 4-9-1.本研究模式之弱點在 OWASP 十大雲端服務風險報告中的對應分類

弱點		在 OWASP 分類
V1	粗略的授權認證與計費系統	T9,T4,T5
V10	不能在加密狀態下處理資料	T9,T4,T5
V13	缺乏技術標準與標準解決方案	T1,T4,T5,T9
V14	沒有原始碼託管協議	T1,T4,T5
V16	沒有控制漏洞評估程序	T1,T4,T5
V17	可能在內部或雲端網路上發生的掃瞄	T7,T4,T5
V18	使用者可能會對鄰居的資源做偵測	T7,T4,T5
V21	合約沒有寫清楚責任歸屬	T1,T4,T5
V22	跨雲端應用程式隱含相依關係	T1,T4,T5
V23	服務水平協議條款可能會在不同利害關係人間產生互斥	T1,T4,T5
V25	雲端服務商無法藉由稽核或認證給予客戶任何保證	T1,T4,T5,T9
V26	認證計畫不適合雲端架構	T1,T4,T5,T9
V29	資料被儲存在多個司法行政區，但在這件事上缺乏透明度	T1,T3,T4,T5,T8,T9
V30	缺少該資料儲存所在司法行政區的相關資訊	T1,T3,T4,T5,T8,T9
V31	使用者條款缺乏完整性與透明度	T1,T4,T5,T9
V34	雲端服務提供商組織裡的角色與責任定義不明確	T1,T4,T5,T9
V35	雲端服務提供組織裡角色職責實行不確實	T1,T4,T5,T9
V36	相關當事人知道太多非必要的細節	T9,T4,T5
V37	不充分的技術實體安全	T9,T4,T5
V38	人為設定錯誤	T9,T6,T4
V39	系統或作業系統弱點	T4,T5,T6,T9
V41	缺乏或很差的持續營運與災難復原計畫	T9,T6,T4
V44	資產擁有權不明確	T1,T4,T5
V46	太少雲端服務商可以供選擇	T4,T5

本研究繪製

表 4-9-2.本研究模式之弱點在 OWASP 十大雲端服務風險報告中的對應分類

V47	缺乏生產者剩餘	T4,T5
V48	應用程式弱點或粗劣的更新檔管理	T9,T4,T5
V5	虛擬化弱點	T7,T4,T5
V6	使用者間缺乏實體資源的獨立	T4,T5,T6,T7,T8,T9
V7	使用者間缺乏商譽的獨立	T7,T4,T5

本研究繪製

接著加總對應弱點分數計算出各個分類弱點分數，再加總各分類弱點分數計算出各個公司相對危險度分數，以廠商 1 為例，依照以下算式計算：

比較組廠商 1 危險度
=T1 類弱點分數+…+T9 類弱點分數
=(V13 分+V14 分+…+V44 分)+…+(V1 分+V10 分+…+V48 分)

T1: OWASP 雲端十大安全風險中第 1 項
V13:本研究採用第 13 個 ENISA 雲端弱點

4.4.2 實驗組與比較組廠商排名比較

本研究模式與 OWASP 十大雲端服務風險報告兩種排名方式的差距都在 2 名以內，顯示出本研究模式能大致辨識出較危險與較安全之雲端服務商(危險度越低者排名越前面)，見表 4-10。

表 4-10.實驗組與比較組廠商排名結果比較

		廠商 1	廠商 2	廠商 3	廠商 4	廠商 5	廠商 6	廠商 7	廠商 8	廠商 9	廠商 10
實驗組	危險度	194.00	185.11	174.46	213.47	154.60	171.48	168.54	142.24	159.14	133.16
	排名	9	8	7	10	3	6	5	2	4	1
比較組	危險度	5092	5562	4062	4598	2464	3547	3023	1226	1892	630
	排名	9	10	7	8	4	6	5	2	3	1
實驗組與比較組排名的差距		0	2	0	2	1	0	0	0	1	0

本研究繪製

為了進一步比較本研究模式與比較組計算服務商危險度，我們列出兩種排名計算式，並展開後寫成以弱點分數為主的多元一次線性函數，以廠商 1 為例分別是比較組的計算式：

比較組廠商 1 危險度
=T1 類弱點分數+…+T9 類弱點分數
=(V13 分+V14 分+…+V44 分)+…+(V1 分+V10 分+…+V48 分)
=[V13*(權重 13)]+[V14*(權重 14)]+…+[V48*(權重 48)]

T1: OWASP 雲端十大安全風險中第 1 項
V13:本研究採用第 13 個 ENISA 雲端弱點
權重 13：算式展開整理後 V13 弱點最後的係數

以及實驗組(本研究模式)之計算式(為縮短算式長度以利觀察僅顯示至小數點後三位示意)：

實驗組廠商 1 危險度
=資產 A1 分數*0.777+…+A20 資產分數*0.792
=(R1 分*0.158+…+R23 分*0.424)*0.777+…+(R3 分*0.384)*0.792
=[(V13*0.643+…+V47*-0.313)*0.158+…+(V29*-0.296+V30*0.209)*0.424]*0.777+…+[(V13*-0.175+…+V18*0.489)*0.384]*0.792
=[V13*(權重 13)]+[V47*(權重 47)]+…+[V18*(權重 18)]

R1:本研究採用 ENISA 雲端風險中第 1 個風險
V13:本研究採用第 13 個 ENISA 雲端弱點
權重 13：算式展開整理後 V13 弱點最後的係數

並計算出兩組弱點權重做比較，為了統一比較組權重數值的變化幅度和比較基準，我們分別對兩組權重做了標準化動作(減各自算術平均再除上標準差)，結果見表 4-11：

表 4-11.實驗組與比較組計算式乘開後弱點權重比較表

	實驗組權重		比較組權重			實驗組權重		比較組權重	
	原數值	標準化後	原數值	標準化後		原數值	標準化後	原數值	標準化後
權重1	2.62	1.482195361	3	-0.13861386	權重29	1.65	0.563214636	6	0.722772277
權重5	0.69	-0.34629206	3	-0.13861386	權重30	1.68	0.59163672	6	0.722772277
權重6	2.96	1.804312316	6	0.722772277	權重31	1.42	0.34531199	4	0.148514851
權重7	0.46	-0.56419471	3	-0.13861386	權重34	0.83	-0.21365567	4	0.148514851
權重10	1.3	0.231623652	3	-0.13861386	權重35	1.83	0.733747141	4	0.148514851
權重13	1.65	0.563214636	4	0.148514851	權重36	0.58	-0.45050637	3	-0.13861386
權重14	1.15	0.089513231	3	-0.13861386	權重37	1.1	0.04214309	3	-0.13861386
權重16	1.05	-0.00522705	3	-0.13861386	權重38	0.96	-0.0904933	3	-0.13861386
權重17	0.53	-0.49787651	3	-0.13861386	權重39	2.07	0.961123816	4	0.148514851
權重18	0.56	-0.46945443	3	-0.13861386	權重41	0.88	-0.16628553	3	-0.13861386
權重21	0.5	-0.5262986	3	-0.13861386	權重44	0.85	-0.19470761	3	-0.13861386
權重22	0.25	-0.763149 3	3	-0.13861386	權重46	0.21	-0.80104541	2	-0.42574257
權重23	0.28	-0.73472721	3	-0.13861386	權重47	-0.54	-1.51159752	2	-0.42574257
權重25	0.32	-0.6968311	4	0.148514851	權重48	2.82	1.671675923	3	-0.13861386
權重26	-0.05	-1.04737014	4	0.148514851					

本研究繪製

如圖 4-3 所見,以上數據繪製成長條圖後發現兩組權重的行為雖然不完全一致，但確實有呈現一定程度相同的趨勢，能夠指出類似的結果。例如權重 6、權重 29、權重 30、權重 39 均能辨識出特別危險的弱點，但是權重 14 到權重 25 中 OWASP 模式(比較組)卻不如本研究模式(實驗組)敏感。

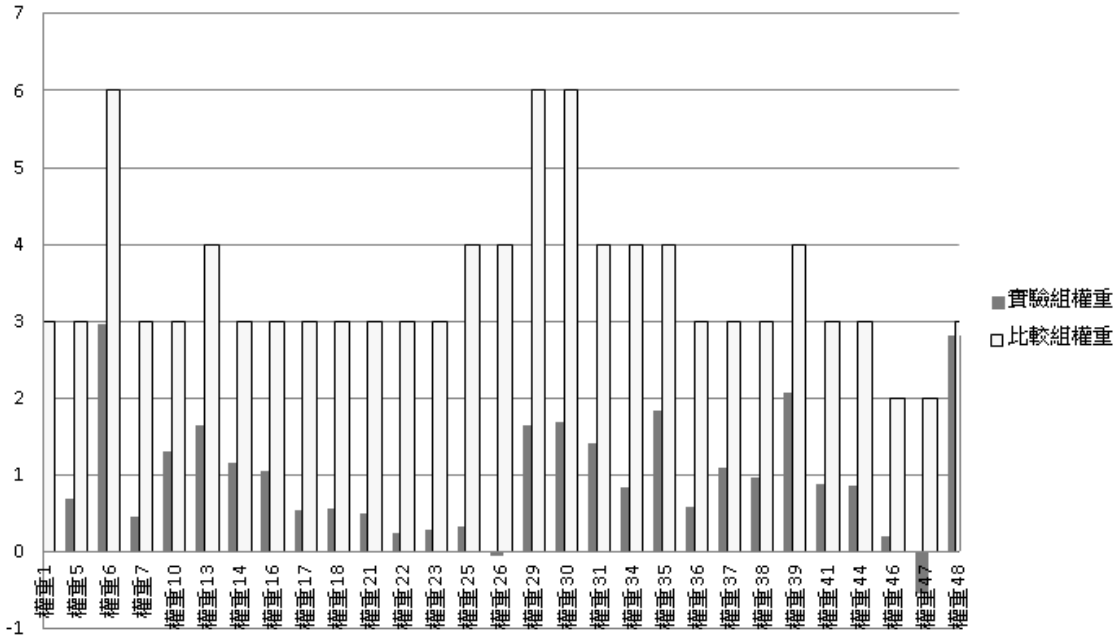


圖 4-3.實驗組與比較組計算式乘開後弱點權重比較圖(未標準化)
本研究繪製

見圖 4-4，如果是以標準化過後的數據繪製圖形可以看得更明顯，權重 6、權重 29、權重 30、權重 39…等弱點權重雖然幅度不盡相同，但都呈現相同的正負趨勢。而權重 17~權重 23 雖然有同樣方向連動趨勢，可是卻無法像本研究提出之模式敏感(實驗組)。但也很明顯觀察到一些不同方向的連動趨勢例如權重 10、權重 25、權重 26、權重 34、權重 37、權重 48。

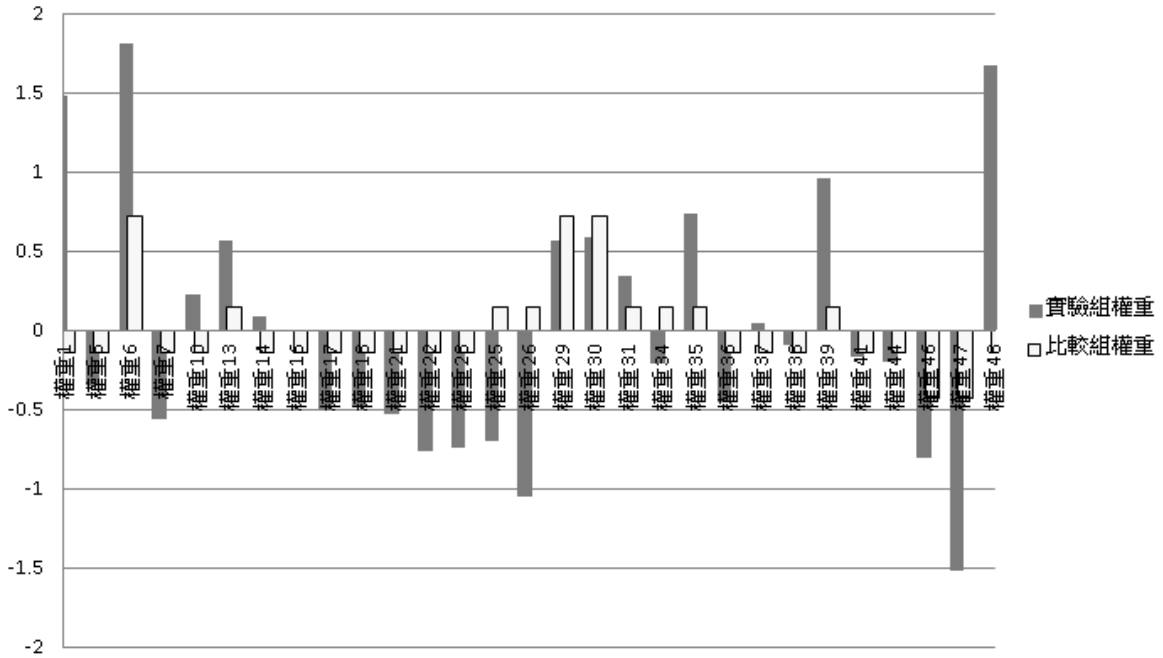


圖 4-4.實驗組與比較組計算式乘開後弱點權重比較圖(標準化)
本研究繪製

4.5 模式應用

本研究所提模式特點是能看出雲端服務高等級風險系統內部的運作結構，計算出結果後還可以回頭觀察弱勢之處並加以改善或因應。首先在建立風險矩陣時要計算風險發生率與風險嚴重度，而如何利用本研究模式計算出發生率與嚴重度則延續 3.2 節之推論。如下式所示意，由弱點對風險關係計算出發生率，由風險對資產及相對危險度計算出嚴重度：

該風險發生率=∑(該風險對應弱點分數)(該風險對應弱點權重)

該風險嚴重度=∑(該風險對資產資產權重)(該資產對相對危險度權重)

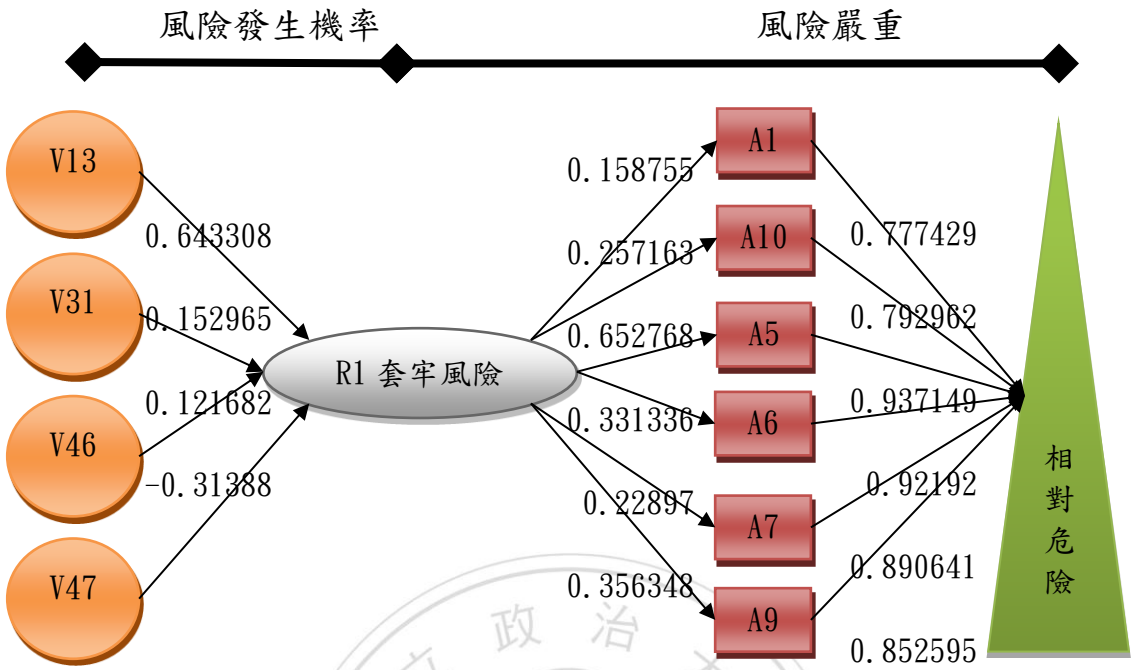


圖 4-5. 風險發生率、風險嚴重度、與本研究模式關係示意(以 R1 為例)

本研究繪製

以計算 R1 風險的發生率與嚴重度為例如下(圖 4-5)：

R1 風險發生率=V13 分數*0.643308+…+V47 分數*-0.31388

R1 風險嚴重度=0.15755*0.777429+…+0.356348*0.852595

R1:本研究採用 ENISA 第 1 個風險

V13:本研究採用 ENISA 第 1 個弱點

接著依此類推就可以計算出九個風險各自風險發生率與嚴重度，這裡再度以廠商 1 的資料為例繪製成下表(表 4-12)，並將發生率及嚴重度分別作為橫軸及縱軸製作出風險矩陣(圖 4-6)：

表 4-12.廠商 1 的風險嚴重度與發生率

風險		發生率	嚴重度
編號	名稱		
R1	套牢	2.408702	1.72699496
R2	失去對資料和系統控制權	24.17121	1.95322432
R3	承諾風險	2.792415	0.30464252
R9	隔離失效	15.66523	1.17166603
R10	惡意的內部員工	21.33588	3.46664434
R26	網路管理風險	12.92346	2.31144425
R21	作為證物或電子蒐證	-2.27579	1.82980016
R22	行政區的風險	8.125036	2.85230834
R23	資料保護處理風險	0.31965	1.80257533

本研究繪製

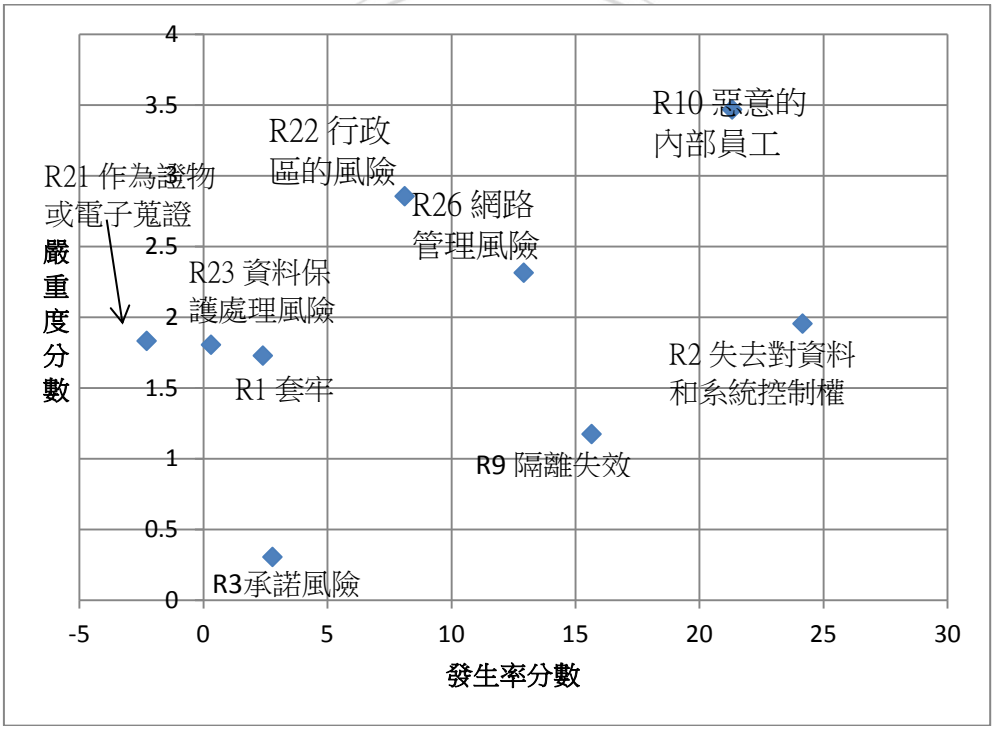


圖 4-6.廠商 1 的風險矩陣圖

本研究繪製

雖然廠商 1 的資料是隨機產生的並不一定可信，但仍然可以利用本研究所提供之模式及風險矩陣工具做一些探討。從廠商 1 的風險矩陣圖看來 R10 內部惡意員工的問題非常嚴重，其他雲端模式最為人擔心的 R2 失去控制權和 R9 虛擬化隔離問題也都很危險。如果我們再加上廠商 2 風險矩陣圖(圖 4-7)一起比較就可以發現廠商 2 的 R10 和 R9

風險較安全，但 R2 風險卻遠險於廠商 1 的 R1 風險。另外從這張圖裡也可以看出以這樣方式分析的風險嚴重度在各公司裡面都是一樣的，因為站在使用者立場不管服務商是誰，同樣資產受損害時造成的危害也相同。

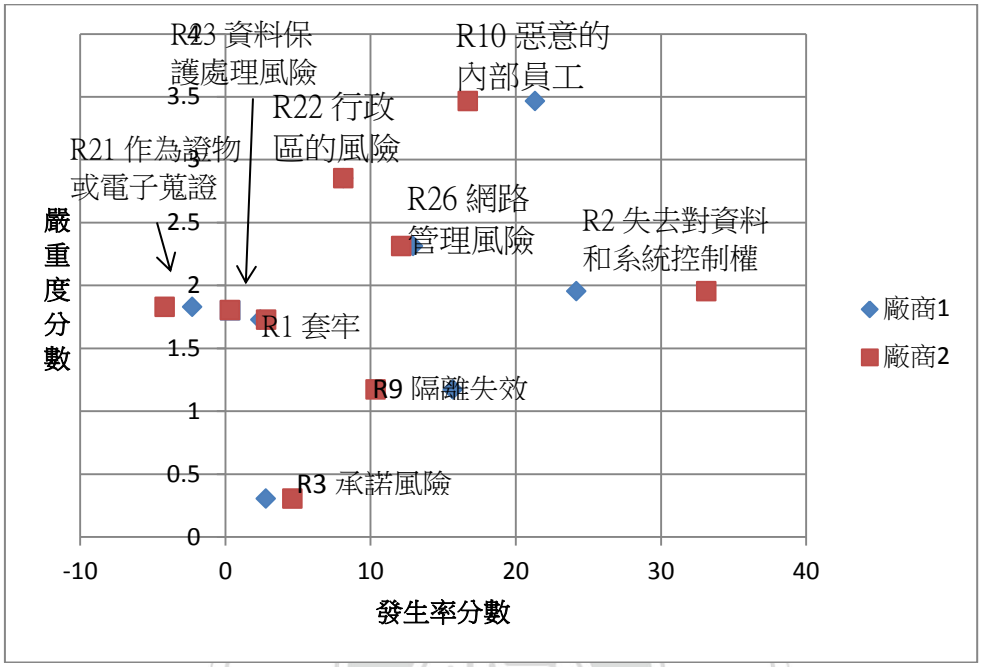


圖 4-7.廠商 1 和廠商 2 的風險矩陣比較圖

本研究繪製

接下來要展示本研究模式的另外一個特色，也就是可以看出其中風險系統運作的結構、追朔到最初造成此危害的弱點、並及早因應獲改善。還是以廠商 1 為例，廠商 1 的相對危險度 194 分，其中最危險的資產是 A2 使用者的顧客信賴 33 分，而最安全的是 A20 認證資產 0.85 分。(表 4-13)

表 4-13-1.廠商 1 的資產對相對危險度分數

資產			權重	相對危險度	
分數	編號	名稱		分數	總計
39.99239	A1	使用者的商譽	0.777429	31.0912448	194.00
41.61024	A2	使用者的顧客信賴	0.793538	33.0193048	
37.97054	A3	使用者的員工忠誠與經驗	0.760062	28.8599608	
13.77741	A4	使用者的智慧財產	0.736031	10.1406007	
24.31379	A5	敏感的個人資料	0.937149	22.7856446	

本研究繪製

表 4-13-2.廠商 1 的資產對相對危險度分數

10.99748	A6	使用者及服務商的個人資料	0.92192	10.1387996	
10.09456	A7	使用者及服務商的關鍵個人資料	0.890641	8.99062757	
5.519912	A8	日常資料	0.922844	5.09401785	
14.77874	A9	需要即時提供的服務	0.852595	12.6002818	
33.29573	A10	服務提供	0.792962	26.4022465	
4.390798	A16	網路	0.91695	4.02614245	
1.072798	A20	認證	0.792962	0.85068834	

本研究繪製

所以把影響 A2 資產的風險拿出來看，發現其中又以 R10 風險 12.68 分的比重最大，第二名 R2 風險 11.75 分也遠大於第三名的 R9 隔離失效風險。(表 4-14)

表 4-14. 廠商 1 的風險對資產分數

風險			權重	資產			
分數	編號	名稱		編號	名稱	分數	小計
21.33588	R10	惡意的內部員工	0.594418	A2	A2 使用者的顧客信賴	12.6824311	41.6102377
24.17121	R2	失去對資料和系統控制權	0.486305	A2		11.7545817	
15.66523	R9	隔離失效	0.278904	A2		4.36909503	
12.92346	R26	網路管理風險	0.556504	A2		7.19195885	
-2.27579	R21	作為證物或電子蒐證	0.10217	A2		-0.23251716	
8.125036	R22	行政區的風險	0.703789	A2		5.71831096	
0.31965	R23	資料保護處理風險	0.395361	A2		0.12637714	

本研究繪製

再把影響 R10 風險的弱點拿出來看，就知道廠商 1 的 V48 應用程式漏洞亟待改善，V48 弱點除了在 R10 風險中最危險外，還具有最大的權重，意味著同樣都改善 1 分安全度時，改善 V48 這項弱點能對 R10 風險有最多改善。(表 4-15)

表 4-15. 廠商 1 的弱點對風險分數

弱點			係數	風險			
分數	編號	名稱		編號	名稱	分數	小計
5	V1	粗略的授權認證與計費系統	0.757214	R10	R10 惡意內部員工	3.78607	21.33588
8	V10	不能在加密狀態下處理資料	0.375566	R10		3.004528	
6	V34	雲端服務提供商組織裡的 角色與責任定義不明確	0.067981	R10		0.407886	
8	V35	雲端服務提供組織裡角色 職責實行不確實	0.214882	R10		1.719056	
2	V36	相關當事人知道太多 非必要的細節	0.168191	R10		0.336382	
6	V37	不充分的技術實體安全	0.317537	R10		1.905222	
10	V39	系統或作業系統弱點	0.36618	R10		3.6618	
8	V48	應用程式弱點或粗劣的更新檔管理	0.814367	R10		6.514936	

本研究繪製

4.6 管理意涵探討

為了進一步分析各個雲端服務風險的發生率和嚴重度權重，我們把所有弱點分數都設定成 1 分(排除個別公司差異，只探討模式權重)如下計算方式：

風險發生率=∑(各風險對應弱點權重)
風險嚴重度=∑(各風險對應資產權重)(對應資產對相對危險度權重)

以套牢風險為例，其對應弱點權重有四個分別是 0.643308、0.152965、

0.121682、-0.31388，所以套牢風險的發生率分數就是這四個數字總和的 0.604075。而同樣的其對應資產的權重有六個，分別乘上各自資產對相對危險度權重，並加總算出 1.726995 作為風險嚴重度的分數。同樣的如同上一節的權重研究，在這裡也做了標準化(減平均、除標準差)。並計算出表 4-16：

表 4-16.各個風險之發生率分數及嚴重度分數

風險		發生率分數		嚴重度分數	
編號	名稱	原數值	標準化後	原數值	標準化後
R1	套牢	0.604075	-0.3536399	1.726995	-0.25111
R2	失去對資料和系統控制權	4.54029	1.17936569	1.953224	0.021375
R3	承諾風險	0.47788	-0.4027881	0.304643	-1.96426
R9	隔離失效	2.391662	0.34255702	1.171666	-0.91997
R10	惡意的內部員工	3.081918	0.61138541	3.466644	1.844212
R26	網路管理風險	1.875892	0.14168428	2.311444	0.452832
R21	作為證物或電子蒐證	-0.31081	-0.7099539	1.8298	-0.12728
R22	行政區的風險	1.034532	-0.1859934	2.852308	1.104275
R23	資料保護處理風險	-0.08656	-0.6226171	1.802575	-0.16007

本研究繪製

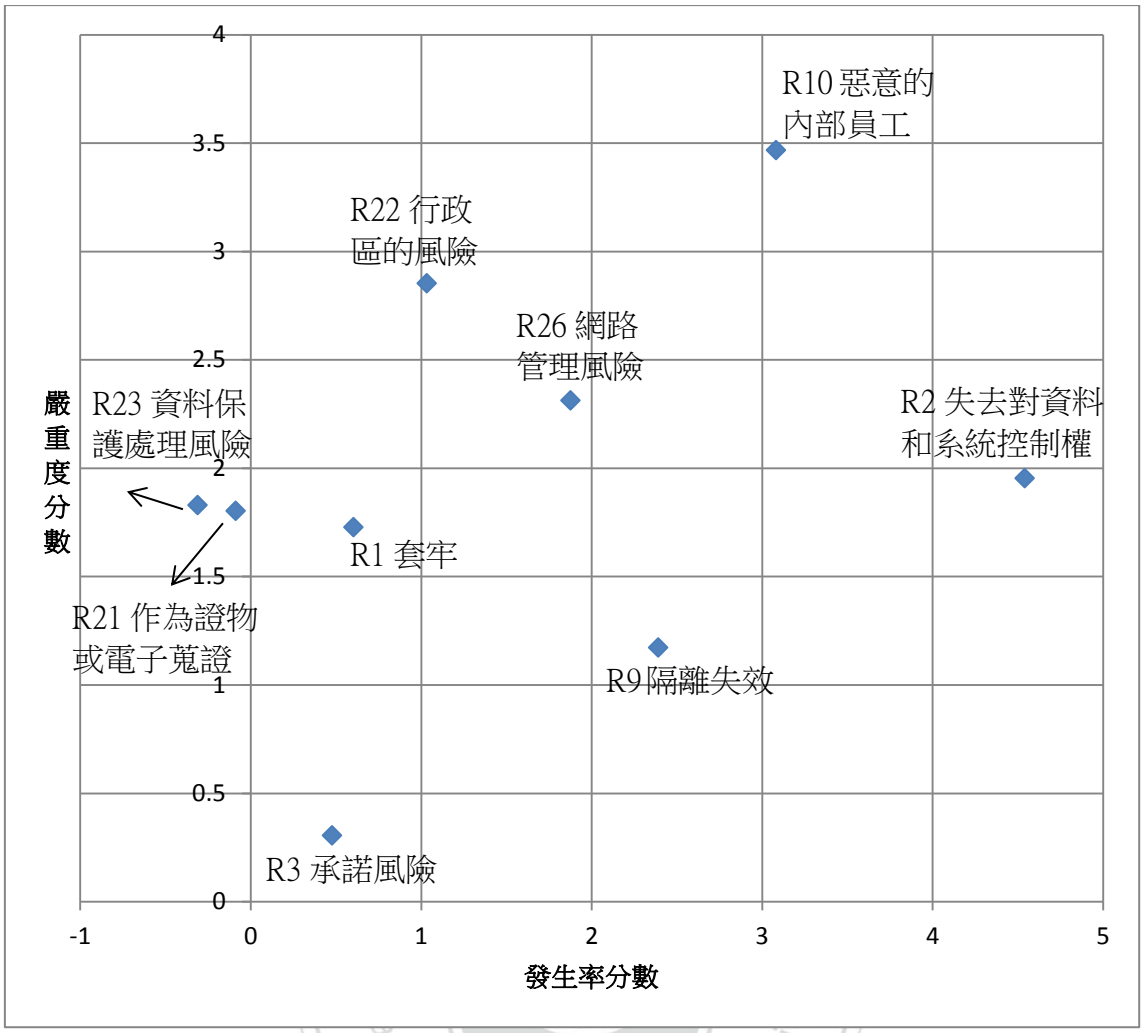


圖 4-8.雲端服務高等級風險權重矩陣(未標準化)
本研究繪製

從圖 4-8 看來企業最擔心的雲端服務風險和傳統資訊系統一樣是人的問題而非技術問題，包含惡意員工、以及失去對資料和系統的控制權，應該要有風險避免及風險轉移動作，並提出適當的危機處理計畫。其次危險的是網路管理、及隔離失效風險，這也是雲端服務模式和傳統資訊架構最不同的地方，需要特別小心設計與處理系統運作機制。而在本研究中企業最不擔心的是資料保護處理、以及作為電子證物或電子蒐證兩個風險項目，很有可能是因為它們屬於有明確法律規範標準且較容易評估的風險項目。

第五章、結論與未來研究方向

5.1 結論

本研究參考歐洲網路與資訊標準組織 ENISA 雲端服務風險報告中 53 項弱點、35 項風險、及 23 項風險，依照報告中的評級萃取出 9 項最高等級風險、29 項風險對應弱點、與 12 項風險對應資產。接著利用問卷及相關係數方式取得並計算出各個弱點、高等級風險、資產、和相對危險度間的相互影響權重建立出一個可以探討因果關係的雲端服務風險評估模式。

然後再利用開放網頁應用程式安全組織(OWASP)的雲端十大安全風險報告計算出另一種雲端服務商風險評估模式與本研究模式的雲端服務商風險排序做比較，發現本研究模式能大致辨識出較危險之雲端服務商與較安全之雲端服務商，且本研究提出之模式更敏感、也提供一個能探討其中風險系統運作狀況的模式或轉化成風險矩陣的表現形式供決策者參考，並能針對有缺失之關鍵弱點做改善。

另外本研究特別針對計算出之風險權重做探討，發現企業最擔心的雲端服務風險項目和傳統資訊系統一樣是人的問題而非技術問題，應該要有風險避免及風險轉移動作，並提出適當的危機處理計畫。其次危險的才是雲端服務模式和傳統資訊系統中較不同的網路管理、及隔離失效風險，需要特別小心設計與處理系統運作機制。而根據本研究結果顯示企業最不擔心的是屬於有明確法律規範標準且較容易評估的風險項目。

5.2 未來研究方向

本研究雖然成功建立出一個敏感且完整的雲端服務風險運作模式，但仍然有很多缺陷之處可以做未來研究改進方向：

1. 問卷度量方式大多是主觀評級，建議能採用更實際之數據資料降低主觀因素、或使用模糊邏輯處理這些主觀評級。
2. 本研究之模式比較僅針對 SaaS 服務模式及公有雲類型，對於其他雲服務模式、雲類型並沒有太多著墨。

3. 雲端服務模式令使用者最擔心的是資料與程式安全問題，因此本研究僅針對雲端服務風險做評分，並未考慮服務商之績效狀況，研究者可建立風險與績效同時考慮之服務商評選模式。
4. 在風險管理五步驟中，本研究只聚焦在風險衡量，對於後續對策選擇、決策實行與績效評估等步驟並沒有太多探討。

參考文獻

中文部分

- 林育震(2010)，『掌控風險 發揮雲端效益』，Communications of the CCISA，16 卷 4 期，138~149 頁
- 張春雄、林顯達、黃新宗、劉美芳(2003)，『風險管理』，吉田出版社
- 陳瑞&周林毅(2007)，『風險評估與決策管理』，五南圖書出版公司
- 黃清賢(2003)，『危害分析與風險評估操作手冊』，新文京開發出版股份有限公司
- 蔡一郎(2010)，『雲端運算與雲端服務風險架構』，Communications of the CCISA，16 卷 4 期，84~93 頁
- 賴世培、詹志禹(2011)，『應用統計(全)』，中華電視股份有限公司

英文部分

- A.Avizienis, J.Laprie, B.Randell.(2000), 'Fundamental concepts of dependability', In Proceedings of the 3rd Information Survivability Workshop
- A.Rosenthal, P.Mork, M.H.Li, J.Stanford, D.Koester, P.Reynolds(2010), 'A new business paradigm for biomedical information sharing', *Journal of Biomedical Informatics*(43:2), pp.324-353.
- IBM(2009), 'Red Book ─ Cloud Security Guidance ─ IBM Recommendations for the Implementation of Cloud Security', IBM
- C.S.Yoo(2011), 'Cloud Computing: Architectural and Policy Implications', *Rev Ind Organ*(38:4), pp.405-421.
- CSA(2010), 'Top Threats To Cloud Computing', Cloud Security Alliance
- ENISA(2009), 'Cloud Computing Security Risk Assessment', European Network and Information Security Agency
- D.Zissis & D.Lekkas(2011), 'Securing e-Government and e-Voting with an open cloud computing architecture', *Government Information Quarterly*(28), pp.239-251.
- European Parliament(1995), 'Directive 95/46/EC of the European Parliament', European Parliament
- L.Iuga(2010), 'The Analysis Of The Correlation Between The Level Of The Bank Fees For Cards And The Number Of Active Cards, Conducted With The Help Of The Pearson Coefficient', Annales Universitatis Apulensis Series Oeconomica(12:1), pp.397-404.

- L.Egghe, L.Leydesdorff(2009), ‘The Relation Between Pearson's Correlation Coefficient r and Salton's Cosine Measure.” *Journal Of The American Society For Information Science And Technology*(60:5), pp.1027-1036.
- L.M.Vaquero, L.Rodero-Merino, D.Morán(2011), ‘Locking the sky: a survey on IaaS cloud Security’ *Computing*(91:1), pp.93-118.
- L.M.Vaquero, L.Rodero-Merino, J.Caceres, M.Lindner(2009), ‘A Break in the Clouds: Towards a Cloud Definition’, *ACM SIGCOMM Computer Communication Review*(39:1), 2009, pp.50-55.
- N.Mayer, P.Heymans, R.Matulevičius(2007), ‘Design of a Modelling Language for Information System Security Risk Management’, *Proceedings of the 1st International Conference on Research Challenges in Information Science(RCIS 2007)*, Ouarzazate, Morocco, April
- NIST SAJACC and BUC Working Groups(2011), ‘NIST US Government Cloud Computing Technology Roadmap Volume III - Technical Considerations for USG Cloud Computer Deployment Decisions’, National Institute of Standards and Technology
- OWASP Cloud Top Ten Project(2012), ‘Cloud Top 10 Security Risks ”, The Open Web Application Security Project
- NIST(2011), ‘NIST Definition of Cloud Computing’, National Institute of Standard and Technology
- G.Purdy(2010), ‘ISO 31000:2009—Setting a New Standard for Risk Management.” *Risk Analysis*(30:6), pp.881-886
- R.K.Chellappa & A.Gupta(2002), ‘Managing computing resources in active intranets’, *International Journal Of Network Management*(12:2), pp.117-128.
- S.Paquette, P.T.Jaeger, S.C.Wilson(2010), ‘Identifying the security risks associated with governmental use of cloud computing’, *Government Information Quarterly*(27:3), pp.245-253.
- T.Schoenherr(2009), ‘LOGISTICS AND SUPPLY CHAIN MANAGEMENT APPLICATIONS WITHIN A GLOBAL CONTEXT: AN OVERVIEW’, *Journal of Business Logistics*(30:2), pp.1-IVV.
- Y.C.Stamatiou, E.Henriksen, M.S.Lund, E.Mantzouranis, M.Psarros, E.Skipenes, N.Stathiakis, K.Stølen(2002), ‘Experiences from using model-based risk assessment to evaluate the security of a telemedicine application’, *Proceedings of Telemedicine in Care Delivery(TICD)*
- L.O.Yusuf, O.Folorunso, A.Akinwale,I.A.Adejumobi(2011), ‘Visualizing and Assessing a Compositional Approach to Service-Oriented Business Process Design Using Unified Modelling Language(UML) ‘, *Computer and Information Science*(4:3), pp.43-59.

雲端運算高等級風險評估問卷

親愛的雲端企業，您好：

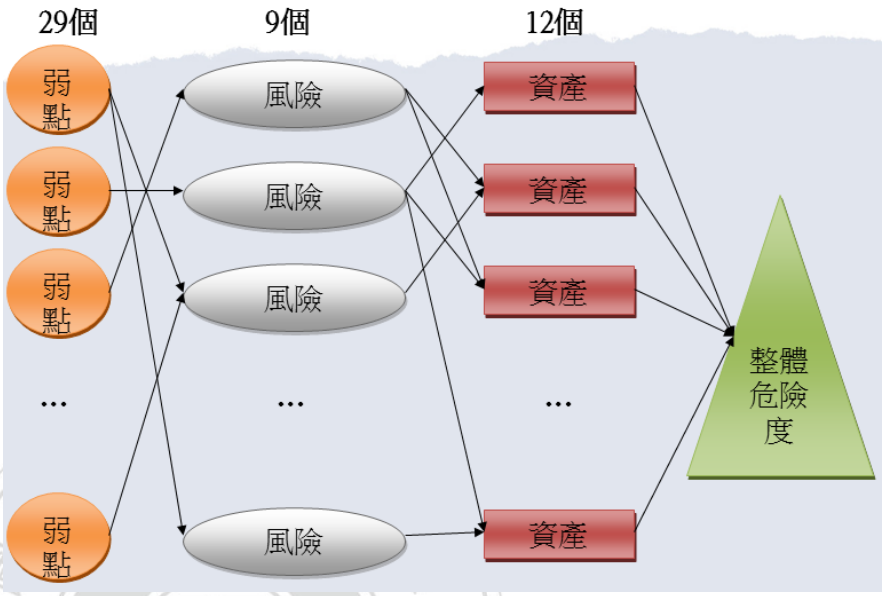
首先感謝您於百忙之中抽空填寫此問卷。我是政治大學資管系研究生，目前正在進行雲端運算風險研究。如下圖所示：弱點造成風險、風險令資產減損，最後間接影響整片雲的危險程度。因此藉由本問卷獲得各個弱點、風險、資產、和整體危險度的評分，再使用統計方法推測它們之間的因果權重。**模型建立完成後，企業主只需對弱點評估就可以推算各個風險發生率、與受害資產狀況，並針對各個風險採取事前因應措施(避免、預防、降低、轉移、承擔)、並作為資安資源分配參考。**

本問卷分為五部分：Part1 風險符合度、Part2 弱點符合度、Part3 資產危險度、Part4 整體危險度、Part5 基本資料。

您的寶貴意見將使本研究更有價值，懇請您能撥出少許寶貴時間，協助完成此研究。

本問卷**所有個別資料不做任何紕漏，唯整體統計結果才做研究使用，敬請安心作答。如果您想獲得研究結果，請在問卷最後自由留下聯絡信箱。**在此謹對您的熱心協助，致上最誠摯的謝意。

敬祝 萬事如意，身體健康！



國立政治大學資管系 科技創新實驗室
指導教授 林我聰 博士
研 究 生 羅邵晏 敬上
98356027@nccu.edu.tw

填寫說明：

1. 若貴公司**具有基礎架構服務提供者(IaaS)身分**，請以使用者觀點客觀評估公司本身提供的雲服務。若**同時具使用者與服務商角色(PaaS、SaaS)**，請以使用者角色填寫。
2. 如果有**無法肯定該填 1 或 10 分、或貴公司服務型態不具該項風險弱點**，請直接填寫 5 或 6 分。

第一部分(Part1)：「題目情境與風險現況」符合程度 請評估「風險現狀與題目狀況」符合程度	完全不同 1	2	3	4	5	6	7	8	9	完全吻合 10
1.我認為使用者被雲端服務商套牢(更換服務商困難)。	□	□	□	□	□	□	□	□	□	□
2.搬上雲端後，得要割讓部分資料和系統控制權給服務商。我認為缺乏對資料和系統的完整安全協議(SLA)。	□	□	□	□	□	□	□	□	□	□
3.我認為服務提供者無法提供他們承認的系統證據(紀錄)，或不允許客戶對他們做稽核。	□	□	□	□	□	□	□	□	□	□
4.我認為因為虛擬化技術的缺失，會令客戶攻擊共同使用同一實體資源的其他客戶。	□	□	□	□	□	□	□	□	□	□

請評估「題目情境與風險現況」符合程度	完全不同 1	2	3	4	5	6	7	8	9	完全吻合 10
5.我認為服務提供商有惡意內部員工(會監守自盜或造成破壞)的存在。	□	□	□	□	□	□	□	□	□	□
6.我認為當某個實體資源被法院查封時，其他租用該資源的客戶會受影響或資料曝光。	□	□	□	□	□	□	□	□	□	□
7.我認為客戶資料位於高風險國家。(資料及系統可能被強迫暴露或充公)	□	□	□	□	□	□	□	□	□	□
8.我認為服務商資料處理過程不合法、不安全、或沒有相關認證。(資料處理、安全活動和資料控制，如：SAS70)	□	□	□	□	□	□	□	□	□	□
9.我認為有網路管理風險。(瀏覽器問題、網路壅塞、連接錯誤、非最佳化使用)	□	□	□	□	□	□	□	□	□	□

第二部分(Part2)：「弱點現況與題目狀況」符合程度 請評估「弱點現況與題目狀況」符合程度	完全不同 1	2	3	4	5	6	7	8	9	完全吻合 10
1.我認為這片雲只透過粗略的授權認證與計費系統就能讓人使用雲端系統資源。	□	□	□	□	□	□	□	□	□	□
2.我認為虛擬化技術弱點。(可能導致實體資源、或另一個虛擬機器被完全控制)	□	□	□	□	□	□	□	□	□	□
3.我認為客戶間缺乏實體資源的獨立。(不同客戶共用同一實體資源)	□	□	□	□	□	□	□	□	□	□
4.我認為客戶間缺乏商譽的獨立。(一個客戶的活動，有可能影響到其他客戶的商譽)	□	□	□	□	□	□	□	□	□	□
5.我認為這片雲不能在加密狀態下處理資料。	□	□	□	□	□	□	□	□	□	□
6.我認為雲端產業缺乏技術標準與標準解決方案。	□	□	□	□	□	□	□	□	□	□
7.我認為缺乏 SEA 協議。(讓使用 PaaS 和 SaaS 服務的客戶在服務商停止服務後，仍然能自行修改與維護系統)	□	□	□	□	□	□	□	□	□	□
8.我認為服務服務商沒有控制漏洞評估程序。(意味著客戶得自己負擔基礎架構安全的責任)	□	□	□	□	□	□	□	□	□	□
9.我認為某一個客戶，可能對其他客戶的內部網路、或雲端網路做掃瞄	□	□	□	□	□	□	□	□	□	□
10.我認為客戶可能會對共用實體資源的其他客戶做偵測	□	□	□	□	□	□	□	□	□	□
11.我認為合約沒有寫清楚責任歸屬(Ex:加密檔案的責任)	□	□	□	□	□	□	□	□	□	□
12.我認為跨雲端應用程式隱含相依關係(開發商擴充服務時，需要依賴雲端服務商的架構支援)	□	□	□	□	□	□	□	□	□	□

請評估「弱點現況與題目狀況」符合程度	完全不同 1	2	3	4	5	6	7	8	9	完全吻合 10
13.我認為服務水平協議(SLAs)可能會和其他利害關係人的承諾或條款產生互斥	□	□	□	□	□	□	□	□	□	□
14.我認為服務商無法藉由稽核或認證給予客戶任何保證	□	□	□	□	□	□	□	□	□	□
15.我認為認證計畫不適合雲端架構	□	□	□	□	□	□	□	□	□	□
16.我認為資料被儲存在多個司法行政區，但在這件事上缺乏透明度	□	□	□	□	□	□	□	□	□	□
17.我認為缺少資料儲存所在地司法行政區的相關資訊	□	□	□	□	□	□	□	□	□	□
18.我認為使用者條款缺乏完整性與透明度	□	□	□	□	□	□	□	□	□	□
19.我認為服務商內部的角色與責任定義不明確	□	□	□	□	□	□	□	□	□	□
20.我認為服務商內部的角色職責實行不確實(可能創造出權力過大的管理員)	□	□	□	□	□	□	□	□	□	□
21.我認為相關當事人知道太多非必要的細節(當事人只要知道原則，而非所有細節)	□	□	□	□	□	□	□	□	□	□
22.我認為技術本身有安全問題，但相關防護並不夠充分(例如：RFID 的資安問題、無防竊聽的電磁保護裝置)	□	□	□	□	□	□	□	□	□	□
23.我認為有人為設定錯誤(不適當的程式「安全設定、僵化程序、人為失誤、未受訓練的管理員)	□	□	□	□	□	□	□	□	□	□
24.我認為系統或作業系統有弱點	□	□	□	□	□	□	□	□	□	□
25.我認為服務商的持續營運與災難復原計畫很差或缺乏	□	□	□	□	□	□	□	□	□	□
26.我認為雲端上的資訊資產擁有權不明確	□	□	□	□	□	□	□	□	□	□
27.我認為太少雲端服務商可以供選擇	□	□	□	□	□	□	□	□	□	□
28.我認為缺乏生產者剩餘(服務商的利潤太少)	□	□	□	□	□	□	□	□	□	□
29.我認為應用程式具有弱點或更新檔管理粗劣	□	□	□	□	□	□	□	□	□	□

第三部分(Part3)：「資產」危險程度 請評估「資產」危險程度	非常安全 1	2	3	4	5	6	7	8	9	非常危險 10
1.我認為客戶的「商譽」非常危險	□	□	□	□	□	□	□	□	□	□
2.我認為客戶的「顧客信賴度」(包含友好度，可以從客訴衡量) 非常危險	□	□	□	□	□	□	□	□	□	□
3.我認為客戶的「員工忠誠與經驗」非常危險	□	□	□	□	□	□	□	□	□	□
4.我認為客戶的「智慧財產」非常危險	□	□	□	□	□	□	□	□	□	□
5.我認為客戶及服務商的敏感的個人資料(意指可以猜測出「人種、宗教、政治傾向、社群成員、商業聯盟」....等，的資料)非常危險	□	□	□	□	□	□	□	□	□	□
6.我認為客戶及服務商的個人資料(任何可以辨識資料出資料擁有者本人(自然人)是誰的資訊 ex:身分證號、身體、生理、心裡、經濟、文化、或社會身份…等)非常危險	□	□	□	□	□	□	□	□	□	□
7.我認為客戶的關鍵個人資料(「組織認為非常重要」的資料)非常危險	□	□	□	□	□	□	□	□	□	□
8.我認為客戶的日常資料(「營運相關但被排除在資料保護範圍外」的資料) 非常危險	□	□	□	□	□	□	□	□	□	□
9.我認為需要「即時提供」的服務非常危險	□	□	□	□	□	□	□	□	□	□
10.我認為「不必要及時」提供的服務非常危險	□	□	□	□	□	□	□	□	□	□
11.我認為網路狀況 (包含「雲內互聯」或「雲內外連接」)非常危險	□	□	□	□	□	□	□	□	□	□
12.我認為資安認證資格會被取消(ISO、PCI DSS……等)	□	□	□	□	□	□	□	□	□	□

第四部分(Part4)：「整體相對」危險程度 請參考 Part3 的「12 項資產」、加上「各資產重要性」考量後，評估「相對於」其他雲端廠商的「危險程度」	非常安全 1	2	3	4	5	6	7	8	9	非常危險 10
1.我認為相對於其他廠商，把「資料和系統」放在目前廠商營運的雲上非常危險	□	□	□	□	□	□	□	□	□	□

第五部分(Part5)：基本資料 **(個別資料只做研究應用，「絕不對外公開」)**

1.請問貴公司使用(或提供)的雲端「服務類型」(可複選) □IaaS □PaaS □SaaS □其他_____

2.請問貴公司使用(或提供)的「雲種類」(可複選) □公有雲 □私有雲 □混和雲 □其他_____

3.請問貴公司使用(或提供)雲服務的「時間」□1 年以下 □1~2 年 □2~3 年 □其他_____

4.請問貴公司是屬於雲端服務「使用者」，還是服務「提供者」？(可複選) □使用者 □提供者

5.請問您在貴公司負責之職務為何？(可複選)

□技術人員 □專案經理(PM) □法務人員 □業務人員 □主管或策略人員 □其他_____

6.請問貴公司使用的「雲端服務廠商」是(如果貴公司是雲端服務提供商請填寫「提供的服務內容」)
(選填)_____

7.若您對本研究有興趣，想獲得後續結果，請留下「e-mail」、及「稱呼」
(選填) _____

8.您想對本研究說的話，或提供之意見
(選填) _____

本問卷到此全部結束，非常感謝您對研究的支持與協助