Communications of the CCISA
Vol. 25 No. 2 May. 2019

教育雲端資訊系統之安全性評估模式

蔡璧如[1]、林鈞浩[2] 、何彥霖[2] 、易穎欣[2] 、張博遠[2] 、洪玄姿[2] 、陳芃婷[3*]
[1]義守大學企管系、[2]高雄大學企管系、[3]成功大學醫工系
[1] pijubea@isu.edu.tw、[3] chen@bme.ncku.edu.tw

摘要

雲端運算正在蓬勃發展，為使用者提供共享軟硬體資源和訊息服務，帶來資訊的互通性、可攜性與行動性，不少國家都積極推動雲端資訊系統並應用在各行各業。雲端資訊系統在教育上帶來不少效益與突破，但雲端資訊系統的安全性一直都是受關注之議題。本研究的目的在了解雲端資訊系統的安全性問題以及教育機構在使用雲端資訊系統時面對的安全疑慮，經過整合與分析，評選出教育雲端資訊系統之關鍵的安全性因素。在研究方法上，本研究第一階段採用內容分析法，透過面對面非結構式專家訪談法訪談教育機構，了解教育機構在使用教育雲端資訊系統上所面對的安全疑慮，第二階段進行文獻回顧以彙整出文獻中所提及的安全性問題，並與第一階段的分析結果統合而歸納出教育雲端資訊系統安全性因素。設計專家問卷，透過模糊德菲爾法進行分析，以門檻值 75.00 評選出 12 個關鍵的安全性因素，建立出教育雲端資訊系統之安全性評估模式，讓教育機構能夠有效地評估教育雲端資訊系統。本研究亦提出提高教育雲端資訊系統之相關建議，期望能夠解決教育機構的安全疑慮，加強教育雲端資訊系統之應用，推動未來創新的教育模式。

關鍵詞：教育雲、雲端運算、雲端安全、內容分析法、模糊德菲爾法

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 25 No. 2 May. 2019

Education Cloud Security Evaluation Model

Pi-Ju Tsai[1], Chun-Hao Lin[2], Yin-Lam Ho[2], Vin-Nhan Ho[2], Po-Yuan Chang[2], Hsuan-Tzu Hung[2], Peng-Ting Chen[3*]
[1]Department of Business Administration, I-Shou University,
[2]Department of Business Administration, National Kaohsiung University of Science and Technology
[3]Department of Biomedical Engineering, National Cheng Kung University
[1]pijubea@isu.edu.tw, [3]chen@bme.ncku.edu.tw

Abstract

Cloud computing is growing quick and well, providing users with shared software and hardware resources and messaging services, bringing information interoperability, portability and mobility. Many countries are actively promoting cloud information systems and applying them in various industries. Cloud information system brings many benefits and breakthroughs in education, but the security of cloud information systems has always been a topic of concern. The purpose of this study is to understand the security issues of cloud information systems and the security concerns that educational institutions face when using cloud information systems. After integration and analysis, the key security factors for educating cloud information systems are selected.

The first phase of the study uses content analysis to deal with the results of interview of educational institutions, to understand the security concerns faced by educational institutions in using education cloud information systems. In the second stage, a literature review was conducted to summarize the safety issues mentioned and integrated with the analysis results of the first phase to summarize the safety factors of the education cloud information system. Third, design expert questionnaire, through fuzzy Delphi method analysis, selected 12 key security factors with a threshold of 75.00, established a security assessment model for education cloud information system, enabling educational institutions to effectively evaluate education cloud information system .

Keywords: education cloud, cloud computing, cloud security, content analysis, Fuzzy Delphi Method

壹、緒論

隨著科技的急速發展，雲端運算成為了新趨勢。雲端運算的主要概念是建構一個虛擬化的計算資源池，藉由集中豐富的運算資源並連接網絡，提供基礎設施、平台、軟件服務[2] ，帶來隨時隨地存取資料、多人共享資源及減少使用者終端負擔等優點。雲端運算可儲存數據與程序，客戶可以透過輕便的行動裝置在任何時間任何地方存取數據，帶來數據流動性,訪問靈活性和應變能力等好處[7] 。雲端資訊系統逐漸應用在教育上，帶來虛擬教室、電子書包及數位學習資源等創新之教育模式，從而打破時間地點限制、讓訊息與資源共享、降低成本以及教學資源整合，提供更多元化的教育模式[19] 。眼見教育雲端資訊系統帶來的創新與效益，美國、英國、中國、泰國、日本等國家都制定相關政策努力推動教育雲端科技發展[13] 。

發展雲端資訊系統當中最大的挑戰在於對使用者提供資訊安全的保證，不論使用公有雲 、私有雲、社群雲或是混合型的雲端服務，都必須面對雲端資訊系統之安全性問題[31] 。雲端安全聯盟(Cloud Security Alliance)指出雲端環境主要面臨七種不同的安全威脅，分別為雲端運算進行非法行為、不安全系統界面、組織內惡意人員、資源非法共享、資料遺失外洩、帳號竊取以及其他未知風險；同樣地，教育機構在使用教育雲端資訊系統時亦帶有疑慮，諸如如何防止機密資料的洩漏、教育資源如何安全地共享、如何保障貢獻者之權益和利益等都是教育機構所必須面對的問題[16] 。由此可見，雲端資訊系統成功與否的關鍵取決於雲端安全性[10] [11] [19] [22] [23] [31] [33] ，在評估雲端環境時，資訊安全成為了首要的考量因素，當中包括了個人資料保護、使用者認證及通訊安全性等管理層面[31] 。

本研究的研究目的為建立教育雲端資訊系統之安全性評估模式，透過下述步驟進行研究：首先確認研究主題及研究目的，然後蒐集國內外關於雲端資訊系統及教育雲端資訊系統之文獻與產業報告,整理出雲端資訊系統相關的安全性問題。透過設計訪談大綱、以面對面非結構式專家訪談法訪談教育機構，採用內容分析法找出教育雲端資訊系統安全性評估因素。將找出的安全性評估因素依據模糊德菲爾法設計成問卷，邀請教育機構內之專家填寫，以辨識出影響教育雲端資訊系統之關鍵的安全性因素，進而建構教育雲端資訊系統之安全性評估模式。

貳、文獻探討

2.1 雲端資訊系統與安全性議題

雲端運算(Cloud Computing)是一種透過網際網路，將軟硬體資源和訊息共享到不同電腦與裝置的運算方式,雲端服務可分為基礎設施層(IaaS)、平台層(PaaS)和應用層(SaaS)三種層次，以及公有雲、私有雲、社群雲以及混合雲四種服務方式，採用不同的服務種

類，面對的雲端資訊安全風險也會有所同[29] 。

雲端安全聯盟於 2009 年成立，旨在推廣雲端安全，並提供雲端安全架構相關資訊，讓使用者在安全的情況下使用雲端系統。雲端安全聯盟於 2009 年發佈第三版雲端安全指引，成為實行雲端服務安全要求的指標，建立雲端安全可分為雲端架構、雲端治理、雲端營運 3 個主要部份，其中又細分成 14 個領域進行評估，分述如下，本研究將依據此指引分類出雲端資訊系統安全性因素。

2.1.1 雲端架構

雲端運算架構框架

了解雲端運算是建置雲端重要的第一步，雲端運算架構框架這個領域是以資訊網路與安全專業人士的獨特角度，描述雲端運算與架構框架，在不同產業上雲端的結構及框架都不一樣，因此企業必須理解雲端的特性、服務模式、部署模式、結構以及框架，才能夠訂定出最適合的雲端系統[1] 。

2.1.2 雲端治理

治理與企業風險管理

良好的雲端治理和企業風險管理應實施適當的組織結構、流程和控制措施，並維持有效的信息安全治理、風險管理和法規遵從性，保證整個信息供應鏈在雲端服務建置者、第三方供應商及客戶三方面的信息安全[1] 。

在雲端治理方面，企業應確保所有雲端相關的策略規劃，當中包括評估、投入及管理時間、人力、資金及設備等資源，都能夠與企業整體的策略保持一致性[25] 。部分使用者可能會透過第三方雲端服務供應商進行伺服器建置與維護，將使用者或顧客之重要資料放在雲端資料庫引起洩漏風險，也會帶來管理以及稽核上的問題[5] [21] 。

在企業風險管理方面，不少企業在使用雲端時因沒有徹底評估導致偏離方向，也有不少企業簡單地認為雲端必然涉及到高風險，深入的風險評估可以解決這些問題[4] 。建置者必須將雲端化產生的相關風險因素納入擬定雲端架構之考量[23] 。不少國家及國際組織都頒發出許多不同類型的風險管理模式，為迎合各種特定的需求，每個模式都擁有不同的目標、步驟、結構和應用，因此企業選擇與引入一個完整的信息安全風險管理模式變得十分重要[7] 。

法律議題：合約與電子證據發現

雲端資訊系統迅速發展，企業逐漸將傳統的資料中心往雲端遷移，客戶和供應商都需要清楚了解現有的法律規範、審計標準、流程等[1] ，例如歐盟隱私法即對於資料有地域性的限制傳輸[22] 。另外，雲端服務供應商除了滿足上市合規認證是最低要求，供應商還應採取積極主動的態度，分享如何安全實現和控制雲端服務、如何解決遇到的問題等[4] 。

資訊管理與資料安全

企業逐漸導入雲端資訊系統，保障隱私權成為雲端服務最受關注的議題。雲端運算有著彈性，多租戶，新架構的特色，雲端安全聯盟建議建置者可透過數據安全管制、數據安全生命週期等方式提高資訊與資料管理的安全性[1] 。另外，企業必須做好資料的彙整及分類，以及確定資料的正確性，提高在雲端服務的安全性[33] 。

當雲端供應商進行伺服器建置與維護時，有時會進入系統，供應商或個別員工將有可能有意或無意地洩漏客戶數據，同時也會帶來稽核管理上的問題[5] [8] [22] 。

相互運作與可移植性

相互運作與可移植性是指雲端服務允許數據和應用程式從一個平台任意地移動到另一個平台，或從一個服務供應商轉移到另一個服務供應商的程度[15] 。若雲端服務欠缺相互運作與可移植性，將會有系統或程序不相容造成服務中斷或應用程序故障、從現有雲端供應商遷移到另一個雲端服供應商的能力被限制等的風險[1] 。

2.1.3 雲端營運

傳統安全、營運持續和災難復原

在傳統上信息安全包括機密性、完整性與可用性三個原則。傳統安全不僅限於入侵的威脅，還包括基礎設備、人員和系統的實質威脅等，為了減輕這些風險，可以採取主動與被動的防禦措施，包括設立安全回應中心阻止駭客攻擊、檢測系統來監控安全[1] 。

雲端營運服務必定要持續，才能為企業帶來穩定且優良的服務系統，並為客戶端增進品質且進一步提高客戶端的滿意度[28] 。

災難復原是指透過備份與復原、當遇上突發情況時，達到資料復原的目標，災難復原必須是在可負擔的成本下將數據可靠保護好，並易於管理。災難復原的解決方案是建立在三個基本原則之下：一個完全可虛擬化的儲存基礎設施、一個緊急回應的自助服務和災難復原應用程序[1] 。

資料中心營運

資料中心(Data Center)是指用於安置電腦系統及相關部件的設施，企業可透過廣設資料中心，在虛擬的環境中進行管理及營運，從而得到彈性運算及即時回應之服務[17] 。在建置資料中心或與選擇供應商時，應清楚了解資料中心運行的過程與任務及選擇正確的數據中心位置選址來持續資料中心營運[1] 。

事故回應

雲端資訊系統日常會受到不同的威脅，建置者不需建立一個全新的雲端事故回應概念框架，而是應透過現存的事故回應方案、流程制定出不同情況的應急預案，應用在不同的特定環境中，並評估出應急事件生命週期，加強雲端系統之事故回應能力[1] 。

另外，雲端資訊系統必需具備自動化應變之能力，透過自主的應變措施，了解雲端系統之風險，並且透過持續的風險評估與改善，使雲端服務得以持續[30] 。在服務自動化的事件中，雲端資訊系統可結合稽核與報表的功能，回應虛擬機器之相關重要事件資

訊[22] 。

應用程式安全

雲端擁有靈活性和開放性的特點，但卻同時對雲端安全造成挑戰，因此雲端系統應用程式的設計至操作，到最終退役都需要完善管理，從而降低雲端的風險，企業可透過以下方法管理應用程式安全[1] ：

- 開發與維護雲端安全軟件
- 將每次受影響的攻擊都記錄在案並評估風險
- 任何時間進行系統監控
- 定期進行滲透測試，並檢查系統漏洞

另外，林育震（2010）則認為在使用雲端平台上，自動建立防護功能為影響應用程式安全之關鍵決定因素。

加密與金鑰管理

雲端系統具備多租戶和管理員的特性，為了分辨適合和不適合取得資訊的使用者，建置者應透過加密資料和金鑰管理的方式加強雲端安全[1] 。

識別、權限與存取管理

使用者在使用雲端系統時可分割成三個獨立的功能，身份、權限和存取管理[1] 。識別身分之技術在雲端中扮演相當重要之角色，若能正確辨認合法使用者，就能強化雲端安全性[8] [15] 。

雲端應具備授權、完整性與隱私性三大安全項目，授權能讓系統分辨各種授權人員，而系統應該確保雲端內的資訊有絕對的完整性，不會被不法修改，另外，雲端系統要確保隱私性，防止未經授權人員存取資料[34] 。當中未經授權人員可分為兩部分，第一為外部敵人，其目的為提取公共雲及私有雲中的機密信息；第二是內部敵人，其目的是在自己的範圍之外可從註銷用戶及其他未經授權的用戶獲得更多的權限(Li, Chen, Liu & Jia, 2014)。

虛擬化

虛擬化是基礎架構作為服務(IaaS)雲服務的關鍵要素之一，同時也是私有雲的一種。其越來越頻繁的被應用在平台作為服務(PaaS)和軟件即服務(SaaS)上[1] 。虛擬化兼具彈性技術以及資源效率分配的優點，結合雲端平台將帶來偌大的效益，但另一方面也會產生資訊安全的隱憂[32] ，造成有形及無形的安全挑戰，例如虛擬化之漏洞與 Web 應用程序之漏洞[10] 。

安全即服務

安全即服務(Security-as-a-Service，SecaaS)是一種以安全性作為雲端服務的外包模式，無需企業自行購買相關硬件，透過高安全專業知識、持續更新病毒庫等，提供以雲端安全為主的服務[1] 。

2.2 教育雲端資訊系統與效益

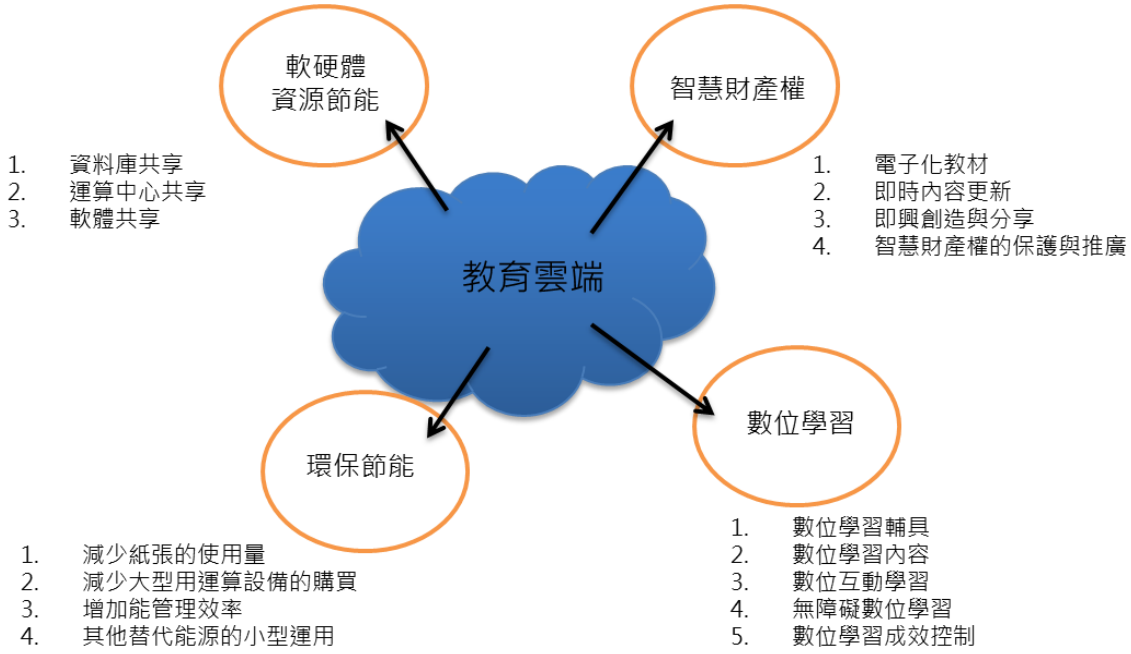
教育雲端資訊系統簡稱「教育雲」，是指將雲端技術應用在教育方面，配合創立虛擬教室、電子書包、數位學習資源等創新的教育模式，提供數位教學服務，讓使用者可以自由自在且自主地學習，不受時間、空間所影響，滿足受到場地、時間限制的使用者之需求，並加入電子元素，從而提升整體學習品質[9] [19] 。黃惟伶（2011）認為教育雲是指透過雲端技術，將教育所需要的東西虛擬化，例如課本、作業、考試卷等。創造一個平台，使學生和老師的溝通更有效率，互動更頻繁，學生可以不受時間限制，隨時隨地地學習。

綜合以上所述，本研究定義教育雲為：「將雲端運算技術應用在教育領域，讓有使用教育資源之需求者能獲得更多資源，並且突破目前教育發展上時空地限制，帶來資訊的互通性、可攜性與行動性」。

使用教育雲的效益，可體現在校園的諸多面向上。在行政方面，可以把學生的資料，會議記錄上傳到雲端。教學方面，可以把教材、講義等教學資料上傳至雲端，實現多媒體遠端教學，例如老師把影片上傳至 YouTube 供學生觀看。在社群方面，學校可以為學生建立一個互動平台，供學生討論、進行社群活動，圖書館共開資訊等。這些都是依靠雲端技術，令學校可以用較少投資獲得較大效益[20] 。

從教育政策的面向看，則建構教育雲端後可有以下四點明顯效益（圖一）：分別為教育相關著作權等的保護與共同創作研究的推動、突破數位學習當前的困難與互動、教育資源的差異分配及綠色教育的成效[18] 。

從上述之例子歸納出教育雲在教育上能夠帶來不少效益，當中包含：打破地點限制線上學習、多元的學習模式、教材更靈活、教師更能因材施教，學生更易吸收知識、訊息與資源共享、降低成本以及整合資源。



圖一、教育雲預期綜效示意圖(資料來源：薛議誠、李世華、游文人，2012)

2.3 教育雲端資訊系統與安全性疑慮

雖然教育雲端資訊系統能夠帶來創新，但不少教育機構對於使用教育雲端資訊系統仍抱有疑慮：

教育機構使用教育雲端資訊系統主要有兩個疑慮：在資訊主導權方面，教育機構使用雲端服務很可能需要由雲端服務供應商承包，資訊環境將有可能被商業公司影響與干擾，教育雲端資訊系統制度並未完善，加上能夠為教育機構提供雲端服務的廠商都屬於大型跨國公司，例如 Google 或 Microsoft 等，如果發生資訊安全事件，教育機構很有可能會求助無門[16] 。

謝佩璇（2012）依據 Mason 於 1986 年提出的四大資訊倫理議題討論發展教育雲可能會面臨的挑戰。第一個議題是隱私，如何保護個人資料及合作成果的資料不外洩。第二個議題是存取，如何隨時隨地安全且穩定的存取資料。第三個議題是財產，隱私性的保全不足時將導致的智慧資本與資產的損失。第四個議題是正確，因雲端是由多人互享的資源池，不同人不同時間點的存取資料將造成重複傳遞而降低正確性。

由上述之文獻顯示目前教育機構對於教育雲端資訊系統在安全上抱有疑慮，主要以資訊安全風險為主，因此本研究將探討教育雲端資訊系統之安全性評估模式。

參、研究方法與實證結果

本研究主要分為兩個階段，第一階段將採用內容分析法，依據雲端安全聯盟所發佈的雲端安全指引作為架構，設計訪談大綱，以分析出雲端資訊系統與教育機構對於使用教育雲端資訊系統之安全因素；第二階段將採用模糊德菲爾法，篩選出教育機構專家在使用教育雲端資訊系統時之關鍵的安全性因素，進而探討教育雲端資訊系統之安全性評估模式，消除與降低教育機構使用教育雲端資訊系統的疑慮，使教育雲端資訊系統能夠更有效的發展。

3.1 第一階段：透過訪談及內容分析法取得並歸納教育雲之安全性因素

3.1.1 訪談內容設計

本研究進行訪談前，將先調查訪談機構的背景資料，包含 1.受訪機構之教玉雲端系統有幾套？其導入年份？2. 教育雲端資訊系統安全性疑慮分別可歸納到雲端架構、雲端治理或雲端營運之哪幾點？3. 受訪機構使用之教育雲端資訊系統分別屬於公用雲／私有雲／混合雲／社群雲哪一種部署模型？4. 受訪機構使用之教育雲端資訊系統分別屬於 IaaS／SaaS／PaaS 哪一種服務模式？

訪談內容包含三大主題：一、整體教育界對於使用教育雲端資訊系統面臨哪些安全性疑慮？可歸納至雲端架構、雲端治理或雲端營運之何項？二、教育機構在使用教育雲端資訊系統面臨哪些安全性疑慮？可歸納至雲端架構、雲端治理或雲端營運之何項？三、教育機構在面對安全性疑慮之因應方法為何？

收回的訪談結果依據內容分析法的步驟進行歸納整理。內容分析是「一種客觀、系統性，以及對於內容定量描述的研究方法」，其目的為確定某些詞彙、概念、主題、短句、字元或文本內的句子，並以客觀的方式量化。「內容」指的是資料的內容，其來源可以為報章雜誌、具研究價值之文稿等。適用於當被研究者提供的口頭訊息對研究本身有決策性作用時，利用內容分析的資料需要完整且正確的訊息，因此可藉由訪談逐字稿進行內容分析[27] 。

3.1.2 內容分析法分析結果

本研究在內容分析法階段訪談了 5 所國立大專院校及 23 所私立大專院校，總計 28 所大專院校（表一）。在國立教育機構中，受訪者背景為資訊相關職務之組長佔 80%，資訊相關職務之專員佔 20%；在私立教育機構中，受訪者背景為資訊相關職務之主任佔 17%，組長佔 44%，專員佔 39%。

採訪內容由 4 名編碼員進行內容分析的編碼歸類工作，編碼員會在當週的研究會議中提出討論，本研究為求學校間標準一致，依據王石番（1991）與 Holsti(1969)提出的信度檢測公式，進行 4 名編碼員的相互同意度及信度檢驗，總結相互同意度為 0.85，總信度為 0.958，已高於學者[2] [24] 所提出之信度標準 0.8 以上，可支持本研究的編碼結果。

表一、受訪教育機構背景統計表

項目		國立教育機構		私立教育機構	
使用者	使用者總人數	63,212 人		230,435 人	
	平均每所大專院校使用者人數	12,642 人		10,018 人	
部署模式	私有雲	100%	總計 100%	95.24%	總計 100%
	公有雲	0%		2.38%	
	混合雲	0%		2.38%	
服務模式	軟體即服務（SaaS）	100%	總計 100%	86.96%	總計 100%
	平台即服務（PaaS）	0%		4.35%	
	基礎架構即服務（IaaS）	0%		8.69%	

資料來源：本研究團隊整理

經過蒐集國內外有關於雲端資訊系統及教育雲端資訊系統之文獻與產業報告，整理出 31 項教育雲端資訊系統相關的安全性因素，再透過內容分析法歸納出教育機構在使用教育雲端資訊系統上的安全疑慮，得到 28 個安全性因素，其中 15 項與文獻重複，有 13 項為文獻中沒有提及的因素。再依雲端安全聯盟發佈之雲端安全指引分為 14 個領域，總計 44 個安全性因素分別歸類如下（表二）。

表二、教育雲端資訊系統安全性因素來源對照表

種類	構面	安全性因素	文獻回顧	內容分析法	引用文獻
雲端架構	雲端運算架構框架	了解教育雲端資訊系統技術	●	●	[1] [29] [37] E
雲端治理	治理與企業風險管理	配合教育雲端資訊系統實施適當的組織結構、流程和控制措施	●		[1] E
		了解使用教育雲端資訊系統之相關風險	●	●	[4] [19] E
		有效的信息安全治理或風險管理機制	●		[1] [34]
		系統雲端化後教育機構整體策略保持一致性	●		[29]
		了解組織對教育雲端資訊系統的需求		●	-
		供應商負責擔保教育雲端資訊系統之風險		●	-
		有效評估教育雲端資訊系統供應商之風險	●	●	[37]

		供應商服務可靠與穩定	●	●	[14]
		有效控管教育雲端資訊系統供應商	●	●	[2]
	法律議題：合約與電子證據發現	政府對教育雲端資訊系統有完整之相關法律規範	●	●	[32] [18]
		與教育雲端資訊系統供應商簽訂明確的服務協議	●	●	[1]
	法規遵循與稽核管理	了解教育雲端資訊系統之相關法律與規範	●	●	[1]
		教育雲端資訊系統供應商主動分享與調查不合法行為或資料	●		[4]
	資訊管理與資料安全	有效保障使用者隱私權	●	●	[5] [7] [17]
		建立數據安全管制	●		[1]
		了解數據安全生命週期	●		[1]
		控管資料安全與時並進		●	-
		員工對個資與隱私有基本認知	●	●	[5] [7] [17]
		控管教育雲端資訊系統供應商員工避免其洩漏客戶數據	●		[5] [7] [17]
		委外後仍可掌握本身的資料	●	●	[18]
	相互運作與可移植性	系統有相容性與可移植性	●	●	[1] [22]
雲端營運	傳統安全、營運持續和災難復原	防止駭客攻擊	●	●	[1] [6]
		建立災難復原機制	●	●	[1]
		建立異地備援機制		●	-
	資料中心營運	廣泛設立資料中心	●		[39]
		了解資料中心運行的過程與任務	●		[1] [39]
		正確的資料中心位置選址	●	●	[1] [18]
		定期更換設備		●	-
	事故回應	制定不同情況的應急預案	●		[1]
		教育雲具備自動化應變之能力	●	●	[18] [34]
	應用程式安全	開發與維護教育雲端資訊系統安全軟體	●		[1]
		將每次受影響的攻擊都留下記錄並評估風險	●		[1]
		任何時間對系統進行監控	●		[1]
		定期進行滲透測試檢查系統漏洞	●		[1]
		建立系統自動防護功能	●		[18]
		教育雲端資訊系統保持高穩定性	●	●	[1]
	加密與金鑰管理	完善的數據加密機制	●	●	[1]
		完善的金鑰管理機制	●	●	[1]

	識別、權限與存取管理	規定使用者帳號密碼複雜度		●	-
		增加更多認證方式識別使用者	●	●	[6] [7] [22]
	虛擬化	解決教育雲端資訊系統虛擬化產生的安全隱憂與漏洞	●	●	[36] [9]
		讓教育雲端資訊系統完全符合虛擬化環境		●	-
	安全即服務	採用安全即服務的外包模式	●		[1] [39]

資料來源：本研究團隊整理

3.2 第二階段：透過模糊德菲爾法專家問卷取得關鍵的安全性因素

3.2.1 問卷設計

第二階段的模糊德菲爾法專家問卷，以文獻回顧與教育機構歸納出使用教育雲端資訊系統之安全性因素，找出教育雲端資訊系統安全性評估模式。

模糊德菲爾法是由 1948 年 Olaf Helmer 所提出的傳統德菲爾法演變而來，其方法主要是想藉由匿名方式取代原有面對面的會議，以此克服在會議中可能會產生組織政治的不良影響[24] 。傳統德菲爾法是一種決策技術，透過多位專家一連串不斷反覆主觀判斷，從而取得相對客觀的結果，經過多次反覆判斷，最後讓多位專家得出一致且可靠性較高的結果，為避免少數專家意見影響多數專家意見，德菲爾法必須讓專家匿名發表意見、不可互相討論及聯繫[24] [25] 。

問卷架構分為四部份，分別是問卷說明、問卷內容、語意尺度表以及受訪者基本資料。由於每位專家對同樣題目在「語意思維」上會略有所不同，因此本研究透過兩階段的評分步驟以求較精確地反映每位專家的評估。首先，請專家評估各安全性因素在「教育雲端資訊系統之安全性的影響程度」上是屬於「極大影響」、「很大影響」、「普通影響」、「很少影響」或是「極小影響」，評估完 44 項安全性因素後，再請每位專家針對上述的五個語意尺度給予 0 至 100 分不等的分數，分數愈高表示愈重要，反之則為愈不重要。譬如某專家認為「供應商服務可靠與穩定」屬於「很大影響」，且認為「很大影響」的最佳分數為 80，而範圍是從 70～90，則將這些數值帶入 FDM 解模糊數後的得分即專家對該安全性因素的評分。

本研究共回收 47 份有效問卷，分別來自 13 所國立教育機構及 34 所私立教育機構。

3.2.2 模糊德菲爾法分析結果

FDM 問卷之安全性因素的得分值總表如下所示(表三)。為了評選關鍵的安全性因素，需設定門檻值。對於門檻值的選擇，不少學者曾進行研究[25] ，認為對於以 0~10 之門檻值，通常會以 6.00~ 7.00 作為門檻值之界定區間，或是採集大值之 60%~80%作為門檻值[28] [29] 。由於本研究之得分值為 0~100，依照文獻所提概念按比例套用，本研究的門檻值則應訂於 60~80 之間，最後決定取 75.00 作為本研究的門檻值，得分值超過 75 以上者列為關鍵的安全性因素。

表三、FDM 分析表

主構面	子構面	安全性因素	得分值	排名
雲端架構	雲端運算架構框架	**了解教育雲端資訊系統技術**	**76.08**	**7**
雲端治理	治理與企業風險管理	配合教育雲端資訊系統實施適當的組織結構、流程和控制措施	71.78	25
		了解使用教育雲端資訊系統之相關風險	72.29	23
		有效的信息安全治理或風險管理機制	73.04	18
		系統雲端化後教育機構整體策略保持一致性	**75.36**	**10**
		了解組織對教育雲端資訊系統的需求	62.86	40
		供應商負責擔保教育雲端資訊系統之風險	**75.48**	**9**
		有效評估教育雲端資訊系統供應商之風險	**77.64**	**4**
		供應商服務可靠與穩定	**79.15**	**1**
		有效控管教育雲端資訊系統供應商	**78.11**	**2**
	法律議題：合約與電子證據發現	政府對教育雲端資訊系統有完整之相關法律規範	74.06	15
		與教育雲端資訊系統供應商簽訂明確的服務協議	**75.36**	**11**
	法規遵循與稽核管理	了解教育雲端資訊系統之相關法律與規範	70.91	28
		教育雲端資訊系統供應商主動分享與調查不合法行為或資料	**75.61**	**8**
	資訊管理與資料安全	有效保障使用者隱私權	74.37	14
		建立數據安全管制	70.66	29
		了解數據安全生命週期	71.07	27
		控管資料安全與時並進	68.35	34
		員工對個資與隱私有基本認知	72.45	21
		控管教育雲端資訊系統供應商員工避免其洩漏客戶數據	**78.07**	**3**
		委外後仍可掌握本身的資料	**75.06**	**12**
	相互運作與可移植性	系統有相容性與可移植性	73.75	16
雲端營運	傳統安全、營運持續和災難復原	**防止駭客攻擊**	**76.30**	**6**
		建立災難復原機制	66.80	36
		建立異地備援機制	69.75	32
	資料中心營運	廣泛設立資料中心	65.30	39

	了解資料中心運行的過程與任務	61.19	42
	正確的資料中心位置選址	60.01	44
	定期更換設備	70.43	30
事故回應	制定不同情況的應急預案	69.67	33
	教育雲具備自動化應變之能力	72.90	19
應用程式安全	開發與維護教育雲端資訊系統安全軟體	72.42	22
	將每次受影響的攻擊都留下記錄並評估風險	70.18	31
	任何時間對系統進行監控	65.62	38
	定期進行滲透測試檢查系統漏洞	66.34	37
	建立系統自動防護功能	72.08	24
	教育雲端資訊系統保持高穩定性	**76.38**	**5**
加密與金鑰管理	完善的數據加密機制	71.54	26
	完善的金鑰管理機制	74.84	13
識別、權限與存取管理	規定使用者帳號密碼複雜度	68.32	35
	增加更多認證方式識別使用者	60.89	43
虛擬化	解決教育雲端資訊系統虛擬化產生的安全隱憂與漏洞	73.06	17
	讓教育雲端資訊系統完全符合虛擬化環境	62.46	41
安全即服務	採用安全即服務的外包模式	72.68	20

註：高於門檻值 75.00，以粗體表示。

資料來源：本研究團隊整理

肆、結論與建議

4.1 結論

本研究蒐集與回顧國內外教育雲端資訊系統相關文獻，並訪談 28 所教育機構之教育雲端資訊系統專家，共歸納出 44 項安全性因素。透過第二階段模糊德菲爾法專家問卷，篩選出 12 項關鍵的安全性因素（請參閱表三），分述如下。

一、雲端架構：雲端運算架構框架

在雲端運算架構框架方面篩選出以下安全性因素：了解教育雲端資訊系統技術（76.08，重要性排名 7）。訪談中有提及此關鍵安全性因素之教育機構有 3 間。當中編號 I 教育機構受訪者就認為由於雲端技術日新月異，目前對於教育雲端資訊系統技術不確定，因此必須仔細了解與評估雲端技術。

二、雲端治理：治理與企業風險管理

在治理與企業風險管理方面篩選出以下安全性因素：系統雲端化後教育機構整體策略保持一致性(75.36，重要性排名 10)、供應商負責擔保教育雲端資訊系統之風險(75.48，重要性排名 9)、有效評估教育雲端資訊系統供應商之風險（77.64，重要性排名 4）、供應商服務可靠與穩定(79.15，重要性排名 1)及有效控管教育雲端資訊系統供應商(78.11，

重要性排名 2)。

在系統雲端化後教育機構整體策略保持一致性方面，雖然在訪談中並未有教育機構提到此關鍵安全性因素，但在學術上認為良好的雲端治理應與教育機構整體的策略保持一致性[31] 。

在供應商負責擔保教育雲端資訊系統之風險方面，訪談中有提及此關鍵安全性因素之教育機構為 C 教育機構，受訪者認為所有的程式難免都有漏洞，若供應商能夠擔保雲端相關風險，可提高教育雲端資訊系統之安全性。

在有效評估教育雲端資訊系統供應商之風險方面，訪談中有提及此關鍵安全性因素之教育機構為 B 教育機構，由於資訊安全問題涉及的層面太大，加上選擇以委外方式建立教育雲端資訊系統，管理者更需評估供應商之風險，目前 B 教育機構已導入資訊安全管理制度，進行風險評估。

在供應商服務可靠與穩定方面,訪談中有提及此關鍵安全性因素之教育機構有 5 所。當中 F 教育機構受訪者指出目前許多學校由於資金問題將學校教育雲端資訊系統採用委外開發方式，供應商服務的可靠度與穩定度將會為學校帶來很大的影響。

在有效控管教育雲端資訊系統供應商方面，訪談中有提及此關鍵安全性因素之教育機構有 4 所。當中 D 教育機構及 S 教育機構受訪者均表示學校需保障教育雲端資訊系統資料之安全，當系統委外或將資料存放在供應商時，學校應確保供應商不會濫用或洩漏重要的資料。

三、雲端治理：法律議題：合約與電子證據發現

在法律議題：合約與電子證據發現方面篩選出以下安全性因素：與教育雲端資訊系統供應商簽訂明確的服務協議（75.36，重要性排名 11)。訪談中有提及此關鍵安全性因素之教育機構有 3 所。在 A 教育機構的個案中，受訪者指出目前不是所有學校對於簽訂服務協議都會提供支援，有時候簽訂服務協議只能靠受訪者個人認知及主管與廠商之間的協調，遇到問題的時候不明確的服務協議將有可能未能保障學校的權益。

四、雲端治理：法規遵循與稽核管理

在法規遵循與稽核管理方面篩選出以下安全性因素：教育雲端資訊系統供應商主動分享與調查不合法行為或資料（75.61，重要性排名 8)。雖然在訪談中並未有教育機構提到此關鍵安全性因素，但在學術上認為目前雲端服務供應商只滿足上市合規認證是不足的[4] ，為提供更安全的雲端服務，供應商應採取積極主動的態度，分享如何安全實現和控制雲端服務、並協助解決遇到的問題等。

五、雲端治理：資訊管理與資料安全

在資訊管理與資料安全方面篩選出以下安全性因素：控管教育雲端資訊系統供應商員工避免其洩漏客戶數據(78.07，重要性排名 4)及委外後仍可掌握本身的資料(75.06，重要性排名 12)。

在控管教育雲端資訊系統供應商員工避免其洩漏客戶數據方面，雖然在訪談中並未有教育機構提到此關鍵安全性因素，但學術上不少學者都有提到控管供應商員工之重要

性，指出供應商員工進行伺服器建置與維護時，有可能有意或無意地洩露客戶數據[8] [21] ，因此對供應商員工之稽核管理十分重要。

在委外後仍可掌握本身的資料方面，訪談中 T 教育機構受訪者認為教育機構將雲端服務委外後經常無法掌握自己本身的資料，最後造成資訊安全問題。

六、雲端營運：傳統安全、營運持續和災難復原

在傳統安全、營運持續和災難復原方面篩選出以下安全性因素：防止駭客攻擊(76.30，重要性排名 6)。訪談中大部分教育機構均認為防止駭客攻擊是重要的安全性因素，在 P 教育機構的個案中，受訪者指出，對於駭客的防護是很難保證的，駭客攻擊的範圍十分廣泛，即使定期進行滲透測試，但仍有可能受到攻擊；在 M 教育機構的個案中，受訪者認為由於駭客攻擊日新月異，其風險是難以預防的。

七、雲端營運：應用程式安全

在應用程式安全方面篩選出以下安全性因素：教育雲端資訊系統保持高穩定性（76.38，重要性排名 5)。訪談中不少受訪者都有提及此關鍵安全性因素，在 F 教育機構的個案中，受訪者認為教育雲端資訊系統保持高穩定性十分重要，但同時指出現今資訊科技變化太快，教育雲端資訊系統隨時都需要進行調整，但在調整的過程中會導致系統穩定性不足，加上系統開發時程一直被壓縮，因此系統保持高穩定性以前困難。

4.2 學術意涵與實務意涵

透過上述之討論，歸納出本研究在模糊德菲爾法上之學術意涵及實務意涵。

一、學術意涵

本研究在文獻回顧及內容分析法的階段，皆引用雲端安全聯盟所發佈之雲端安全指引作為架構，歸類從上述階段所歸納出之安全性因素，本研究與不少學者均認為雲端安全聯盟所發佈之雲端安全指引十分全面與專業，可應用於各行各業。經過模糊德菲爾法歸納出 12 項關鍵安全性因素，12 項因素分別出現在雲端安全指引的 7 個構面中，本研究建議日後研究教育雲端資訊系統安全性之學者，可根據本研究結果，更著重於研究上述 7 個構面，深入探究出提高教育雲端資訊系統安全性之方法。

二、實務意涵

經過文獻回顧、內容分析法及模糊德菲爾法進行分析，本研究找出 12 項教育雲端資訊系統之安全性關鍵因素，在實務上，本研究建議教育機構可根據本研究結果進行教育雲端資訊系統安全性評估，了解目前雲端資訊系統的安全程度，進而改善安全性，使教育雲端資訊系統在安全性上更為完善。

4.3 建議

本研究發現教育雲端資訊系統存在著安全性問題，建議教育機構可參考本研究找出之關鍵因素，對自身之教育雲端資訊系統進行評估，若發現有安全性不足之情況，以下是本研究引用學者之建議及教育機構遇到該安全性問題之因應方法，可供參考。

一、「了解教育雲端資訊系統技術」,在導入雲端服務之前,必須先了解雲端運算的特性、組織策略與目標的改變。另外還要對業務及使用特性分類,確保雲端化能夠精準地達成組織之目標與需求[27] 。在訪談中,K 教育機構就曾面對不了解雲端資訊系統技術的情況,在發現問題後,透過參考供應商與同業,逐漸解決教育雲端資訊系統技術的問題。

二、「系統雲端化後教育機構整體策略保持一致性」,企業應確保所有雲端相關的策略規劃,當中包括評估、投入及管理時間、人力、資金及設備等資源,都能夠與企業整體的策略保持一致性,才能提高雲端資訊系統之安全性[32] 。

三、「供應商負責擔保教育雲端資訊系統之風險」,C 教育機構受訪者擁有與供應商的經驗,他認為所有的程式難免都有漏洞,因為建議教育機構應要求供應商擔保雲端資訊系統之相關風險。

四、「有效評估教育雲端資訊系統供應商之風險」,組織在將儲存與管理資料的工作轉嫁至雲端服務供應商前,應先完整評估供應商[40] ,不少學者對於導入雲端資訊系統方面作出研究,教育機構可將其作為參考。

五、「供應商服務可靠與穩定」,雲端服務供應商應採取積極主動的態度,分享如何實現安全和控制雲端服務,教育機構可訂立明確的服務準則,要求供應商需達到合理的服務穩定度,從而評估供應商的可靠性[4] 。

六、「有效控管教育雲端資訊系統供應商」,大部分受訪者均認為有效控管教育雲端資訊系統供應商是十分重要的安全性因素,B 教育機構受訪者建議,學校將資料存放在系統供應商時前,應確保能夠有效控管服務供應商,否則學校將面對很大的資訊安全風險。

七、「與教育雲端資訊系統供應商簽訂明確的服務協議」,為了保障供應商和消費者雙方的利益,在簽訂服務協議時,雙方可制定一個標準化的安全框架及指定提供方式和地點[12] 。

八、「教育雲端資訊系統供應商主動分享與調查不合法行為或資料」,不少受訪教育機構均認為,供應商的主動性是選擇是否繼續使用其服務的其中一個因素,教育機構可要求供應商在遇到不合法行為或資料時,需協助調查相關行為,同時因應供應商的願意與積極性進行評估,作為選擇供應商的其中考慮因素之一。

九、「控管教育雲端資訊系統供應商員工避免其洩漏客戶數據」,進行雲端管控時,為避免內部的安全威脅,應強化系統之出入控管及設備防護,避免供應商員工洩漏客戶數據,並定期追蹤內部離職員工,再透過確實的教育訓練提升員工之警戒意識,提高雲端資訊系統的安全性[15] 。

十、「委外後仍可掌握本身的資料」,T 教育機構指出教育機構將雲端服務委外後經常無法掌握自己本身的資料,造成資安問題,因此,教育機構將雲端服務委外前,應先評估自身資料的重要性,並與供應商訂立能夠保障雙方的協調,讓教育機構在委外後仍可掌握本身的資料。

十一、「防止駭客攻擊」，駭客入侵是常見的安全性問題，在訪談的過程中，大部分受訪者均認為防止駭客攻擊對於教育雲端資訊系統之安全性十分重要，在 F 教育機構的個案中，受訪者指出F教育機構的雲端系統每天都一直受到攻擊，因此會特別注意，並監察這些 IP 的動作。R 教育機構同樣指出，該校之教育雲端資訊系統經常受到攻擊，因此透過建置防火牆、入侵系統防禦機制等方式降低風險。雲端安全聯盟（2009）認為可以透過設立安全回應中心及檢測系統等防禦措施為降低駭客入侵的風險[1] 。

十二、「教育雲端資訊系統保持高穩定性」，不少教育機構都期望其教育雲端資訊系統保持高穩定性，在 P 教育機構的個案中，受訪者提到該校剛建置教育雲端資訊系統時系統並不穩定，後來透過聘請專業廠商協助解決。雲端安全聯盟（2009）指出可透過開發與維護雲端安全軟件、將每次受影響的攻擊都記錄在案並評估風險、任何時間進行系統監控等方式提高教育雲端資訊系統之穩定性[1] 。

總括而言，本研究給予未來研究之建議為，經由本次研究發現之教育雲端資訊系統安全性因素，是經過文獻回顧與訪談得出，包含學術上及實務上之安全性因素，值得後續學者參考。本研究建議將來學者可更深入之分析，找出更多提高該安全因素之辦法。

最後，本研究在過程中發現，各教育機構在實務上都有將投放資源在不同部分的考量，目前本研究只建立出教育雲端資訊系統之安全性評估模式，未來本研究期望能夠繼續深化，研究出教育雲端資訊系統投放資源於各安全性因素之比例及權重，逐步建立出更完整之教育雲端資訊系統架構，解決雲端資訊系統之安全性問題。

參考文獻

[1] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Security. V3.0*, 11-14. 2009.

[2] J. H. Che, Y. Duan, T. Zhang, and J. Fan, “Study on the Security Models and Strategies of Cloud Computing,” *Procedia Engineering*, 23, pp. 586-593, 2011.

[3] G. Gerbner, (1969). “Cultural indicators: The third voice,” *Communication technology and social policy*, New York: John Wiley, 1969.

[4] C. Jenkins, “The Three Pillars of a Secure Hybrid Cloud Environment,” *Computer Fraud & Security*, 6, pp. 13-15. 2013.

[5] S. Khaled, M. Jose, C. Alcaraz, B. B. Jorge, M. Juan, P. Marín, and Z. Sherali, “Analyzing the Security of Windows 7 and Linux for Cloud Computing,” *Computers & Security*, 34, pp. 113-122, 2013.

[6] J. W. Li, J. Li, X. F. Chen, X. L. Liu, and C.F. Jia, “Privacy-preserving Data Utilization in Hybrid Clouds,” *Future Generation Computer Systems*, 30, pp. 98-106. 2014.

[7] M. D. Ryan, “Cloud Computing Security: The Scientific Challenge, and a Survey of Solutions,” *The Journal of Systems and Software*, 86, pp. 2263–2268, 2013.

[8] S. Stein, J. Ware, J. Laboy, and H. E. Schaffer, "Improving K-12 Pedagogy via a Cloud Designed for Education," *International Journal of Information Management,* vol. 33, no. 1, pp. 235-241, 2012.

[9] D. Sun, G. Chang, L. Sun, and X. W. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," *Procedia Engineering*, 15, pp. 2852-2856, 2011.

[10] 王石番，*傳播內容分析法：理論與實證*。臺北市：幼獅，1991。

[11] 王平、林文暉、郭溥村、王子夏、盧永翔，"雲端運算服務之資安風險與挑戰"，*資訊安全通訊*，16，頁 45~65，2010。

[12] 古亞薇，*教育應用科技產品發展契機*，產業情報研究所（MIC），2012。

[13] 朱敬一，"雲端運算之風險管理：網路、資安與企業運作"，*內部稽核特刊*，頁 29~30，2013。

[14] 周祝瑛、劉豫敏，"雲端教育"，*教育研究月刊*，26，頁 125~138，2012。

[15] 余鑑、呂俊毅，"雲端運算及無所不在學習對公部門發展數位學習的啟示"。*T&D 飛訊*，91，頁 1~15，2010。

[16] 余顯強，"淺談雲端運算在圖書館服務之應用"，*國立成功大學圖書館館刊*，20，頁 1~17，2011。

[17] 林志達，"適用雲端運算之單一登入平台架構"，*資訊安全通訊*，16，頁 173~179，2010。

[18] 林育震，"掌控風險發揮雲端效益"，*資訊安全通訊*，16，頁 138~149，2010。

[19] 洪長宏，"如何確保雲端架構運作之安全性 - 以縮減風險案例探討"，*電腦稽核*，26，頁 115~120，2012。

[20] 徐村和，"模糊德菲層級分析法"，*模糊系統學刊*，4，頁 59~72，1998。

[21] 徐慧民、衛萬明、蔡佩真，"應用分析網路程序法於建設公司住宅企劃方案優先順序選擇之研究"，*中華民國建築學會建築學報*，62，頁 49~74，2007。

[22] 陳廷煌，"雲端服務系統的文件交換分享風險管控"，*資訊安全通訊*，17，頁 62~80，2010。

[23] 陳昭宏，"創業投資公司投資高科技產業模糊多準則評估之研究-以生物科技產業為例"，*輔仁管理評論*，9，頁 87~110，2002。

[24] 陳聖棋、黃永亭，"企業資訊系統採用雲端運算之設計研究"，*電腦稽核期刊*，27，頁 24~28，2013。

[25] 張元杰、史欽泰、簡文強、柯盈兆，"國家型研發計畫評估：企業研發總部觀點"，*科技管理學刊*，14，頁 1~28，2009。

[26] 梁連文、李桐豪、黃博怡，"台灣銀行整併績效之探討 - 模糊德菲法之應用"，*台灣金融財務季刊*，11，頁 31~65，2010。

[27] 梁連文、鍾宇軒、施光訓，"我國農企業資金融通機制之再造"，*會計與財金研究*，

1，頁 33~46，2011。
[28] 楊孝濚，“我國犯罪問題社會經濟因素的逐級迴歸分析”，*社會變遷中的犯罪問題及其對策研討會論文集*，台北：政治大學，1982。
[29] 黃永婷、魏良曲，“雲端治理框架初探”，*電腦稽核期刊*，26，頁 100~107，2012。
[30] 黃惟伶，“雲端時代教育雲－解決教學資源不均問題”，*Ectimes 電子商務時報*，2011。
[31] 黃國彥，*教育大辭書*。國家教育研究院，http://terms.naer.edu.tw/detail/1302710/ (2010)。
[32] 蒲樹盛，“創新科技環境下的資訊管理重點 - 雲端資訊安全、個資隱私保護、營運持續服務”，*品質月刊*，46，頁 22~25，2011。
[33] 維基百科，https://zh.wikipedia.org/wiki/雲端運算 (2019/3/11)
[34] 蔡一郎，“雲端運算與雲端安全架構”，*資訊安全通訊*，16，頁 84~93，2010。
[35] 蔡一郎，“雲端安全與通訊架構研究”，*資訊安全通訊*，18，頁 62~68，2012。
[36] 蔡天浩、陳彥仲、黃秀娟、黃培銘、周國森，“一種應用於虛擬平台之實體隔離機制”，*資訊安全通訊*，17，頁 52~61，2011。
[37] 劉家驊、洪士凱，“雲端運算資料安全防護機制之研究”，*電腦視覺、影像處理與資訊技術研討會*，頁 100~109，2010。
[38] 賴森堂，“降低電子商務個人資料風險的安全事件偵測機制”。*電腦稽核期刊*，29，pp. 49~58，2014。
[39] 薛夙珍、邱亭儒，“行動雲端書櫃之應用服務”，*資訊科技國際期刊*，7，頁 1~12，2013。
[40] 薛義誠、李世華、游文人，“雲端科技在教育上的運用”，*教育研究月刊*，216，頁 19~28，2012。
[41] 謝佩璇，“教育雲端發展現況與挑戰”，*教育研究月刊*，26，頁 57~72，2012。