植基於雲端安全之數位證據鑑識標準作業程序之探討

林宜隆	伍台國	周瑞國
中央警察大學資管系	國防管理學院資管系	國防管理學院資管系
教授	教授	研究生
paul@mail.cpu.edu.tw	w13464@yahoo.com.tw	noking10@gmail.com

摘要

雲端運算發展，百家齊鳴，各廠商主要都在強調其靈活運用，但在宣傳自家產品或服務的同時，很少聽到關於雲端運算衍伸出的資料安全防護議題，資料安全性以及企業用戶對隱私洩露的擔心，此為雲端運算發展亟需克服的關鍵問題。

而數位鑑識(Cyber Forensics)，爰引自犯罪偵查技術，就是在資訊犯罪發生後以科學的方法蒐集、檢驗、分析數位證據(Digital Evidence)，藉以證明犯罪事件之發生及被害者、犯罪者、證物、地點之間的關係[5]，致使數位證據，在犯罪偵辦過程中，具有證據能力及證明力。

本研究的目的為透過雲端運算架構、應用及安全威脅議題進行探討，並針對雲端安全聯盟(CSA)所提出的12個雲端安全的關注領域，對應林宜隆教授的提出PLSE Model[1](Policy、Law、Security、Education)模型的四個面向(政策面、法律面、安全技術面、教育面)，探討CSA Control Matrix的基本安全規則，對雲端服務進行風險安全性評估問題之探討。

雲端安全服務進行風險評估及標準規範，並與數位證據鑑識標準作業程序對映及相關應用探討，進而提出於雲端安全之數位證據鑑識標準作業程序(CCS-DEFSOP)，進一步可提供已導入或通過ISO/IEC 27001企業組織及政府機關面對未來雲端運算環境之安全服務評估參考資料或檢查項目(Checklist)。

關鍵詞：數位鑑識、數位證據鑑識標準作業程序、雲端安全、風險安全性評估

1. 前言

隨著網際網路高速發展下，硬體效能與行動裝置的高速運算需求提升，加上寬頻的普及等面向，來觀察雲端運算的演進，可以從早期的網路撥接(Modem)談起，歷經網路伺服器(Web Server)、主機代管(Web Hosting)、到現今發展的應用服務提供商(Application Service Provider，ASP)。未來的資訊產業中，網際網路服務將是主流，於是雲端運算的概念順應而生。最簡單的雲端運算技術在 網路服務中已經隨處可見，例如「搜尋引擎、網路信箱」等，使用者只要輸入簡單指令即能得到大量資訊。未來如智慧型手機(Smart Phone)、衛星導航(Global Positioning System，GPS)等行動裝置都可以透過雲端運算，發展出更多的應用服務[20]。

資訊科技進步，電腦應用日益廣泛，伴隨而來的資訊安全事件亦成為各界注目的焦點。這些包含駭客入侵與攻擊、惡意破壞、損壞設備等資訊安全事件的發生，可能會造成組織或單位不同程度的損失，若資訊安全事件的發生涉及人為的惡意行為，這就可能形成了「電腦犯罪」[19]。

2. 文獻探討

2.1 雲端運算架構及應用

雲端運算，所謂「雲端」其實就是泛指「網路」，名稱來自工程師在繪製示意圖時，常以一朵雲來代表「網路」。因此，「雲端運算」用白話文講就是「網路運算」。舉凡運用網路溝通多台電腦的運算工作，或是透過網路連線取得由遠端主機提供的服務等，都可以算是一種「雲端運算」。

根據美國國家標準技術研究院(National Institute of Standards and Technology，NIST)定義，雲端運算使用無所不在、便利、隨需應變的網路，共享廣大的運算資源(如網絡、伺服器、儲存、應用程式、服務)，可透過最少的管理工作及服務供應者互動，快速提供各項服務[15]。

雲端安全聯盟(Cloud Security Alliance，CSA)[23]安全指南早期在編寫時，美國國家標準技術研究院(NIST)的科學家還沒有開始定義雲端運算。NIST 給雲運算定義了五個關鍵特徵、三個服務模型、四個部署模型[10]，如圖 1 所示。

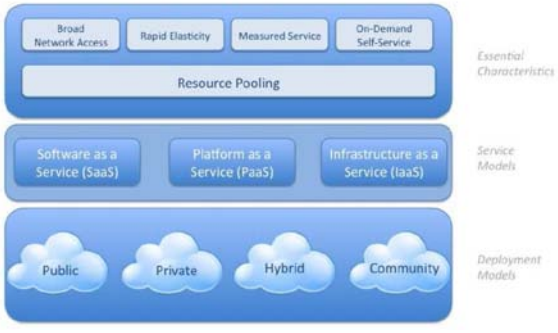

圖 1 NIST 雲端運算定義的形象模型

2.1.1 雲端運算的關鍵特徵

雲端服務展現出的五個關鍵特徵，代表了它與傳統計算方法的關係和區別：

(1) 按個自需求服務(On-Demand Self-Service)：使用者可以在需要時自動配置計算能力，例如伺服器時間和網路存儲的需要自動計算能力，而無需與服務供應商的服務人員交互。

(2) 寬頻接入(Broad Network Access)：透過網路提供的服務能力，支援各種標準接入介面，包括各種客戶端平台(例如行動電話、筆記型電腦、或 PDA)，也包括其它傳統或基於雲端的服務。

(3) 虛擬化的資源“池” (Resource Pooling)：提供商的計算資源彙集到資源池中，使用多租戶模型，按照使用者需要，將不同的物理和虛擬資源動態地分配或再分配給多個消費者使用。雖然存在某種程度上的位置無關性，也就是說用戶無法控制或根本無法知道所使用資源的確切物理位置，但是原則上可以在較高抽象層面上來指定位置(例如國家、州、省、或者資料中心)。資源的例子包括存儲、處理、記憶體、網路頻寬以及虛擬機等。

(4) 快速彈性架構(Rapid Elasticity)：服務能力在某些情況下可以自動地快速、彈性地供應；實現快速擴充、快速上線。對於使用者來說，可供應的服務能力近乎無限，可以隨時按需求購買。

(5) 可測量的服務(Measured Service)：雲端系統之所以能夠自動控制優化某種服務的資源使用，是因為利用了經過某種程度抽象的測量能力(例如存儲、處理、頻寬或者活動用戶帳號等)。人們可以監視、控制資源使用、並產生報表，報表可以對提供商和用戶雙方都提供透明化。

2.1.2 雲端運算的服務模型

NIST 的雲端運算定義共有三種的服務類型，可以分為軟體即服務(Software as a Service)、平台即服務(Platform as a Service)和基礎架構即服務(Infrastructure as a Service)，如圖 2 所示[22]。

(1) 軟體即服務(SaaS)：消費者使用應用程式，但不掌控作業系統、硬體或運作的網絡基礎架構。

(2) 平台即服務(PaaS)：消費者使用主機操作應用程式。消費者掌控運作應用程式的環境(也擁有主機部分掌控權)，但並不掌控作業系統、硬體或運作的網絡基礎架構。平台通常是應用程式基礎架植

(3) 基礎架構即服務(IaaS)：消費者使用「基礎運算資源」，如處理能力、儲存空間、網絡元件或中介軟體。消費者能掌控作業系統、儲存空間、已部署的應用程式及網絡元件(如防火牆、負載平衡器等)，但不掌控雲端基礎架構。

圖 2 Cloud Computing 三種雲端服務圖

2.1.3 雲端運算的部署模型

不管利用了哪種服務模型(SaaS、 PaaS、或 IaaS)，存在四種雲服務部署模型，以及用以解決某些特殊需求而在它們之上的演化變形[15]。

(1) 公用雲：公用雲服務可透過網 路及第三方服務供應者，開放給客戶使用，「公用」一詞並 不一定代表「免費」，但也可能代表免費或相當廉價，公用雲並不表示使用者資料可供任何人查看，公用雲供應者通常會對使用者實施使用存取控制機制，公用雲作為解決方案，既有彈性，又具備成本效益。

(2) 私有雲：私有雲具備許多公用雲環境的優點，例如彈性、適合提供服務，兩者差別在於私有雲服務中，資 料與程序皆在組織內管理，且與公用雲服務不同，不會受到網絡頻寬、安全疑慮、法規限制影響；此外，私有雲服務讓供應者及使用者更能掌控雲端基礎架構、改善安全與彈性，因為使用者與網絡都受到特殊限制

(3) 社群雲：社群雲由眾多 利益相仿的組織掌控及使用，例如特定安全要求、共同宗旨等。社群成員共同使用雲端資料及應用程式。雲端基礎架構由若干個組織分享，以支援某個特定的社區。社區是指有共同訴和追求的團體(例如使命、安全要求、政策或合規性考慮等)。

(4) 混合雲：雲基礎設施由兩個或多個雲(私有雲、社群雲、或公用雲)組成，獨立存在，但是通過標準的或私有的技術綁定在一起，這些技術促成資料和應用的可移植性混合雲結合公用雲及私有雲，這個模式中，使用者通常將非企業關鍵資訊外包，並在公用雲上處 理，但同時掌控企業關鍵服務及資料。

在市場產品消費需求越來越成熟的過程中，將會出現其它的雲端部署模型，意識到這一點很重要。這方面的一個例子就是虛擬專用雲(virtual private clouds)- 以私有或半私有的形式來使用公用雲端基礎架構 ，通常通過虛擬專網 VPN 將公用雲裡的資源連回使用者資料中心內部的資源。

因不同的使用者對於資訊安全、監督管理方式、系統可靠性等要求不同所致[18]，如表 1 所示。

表 1 雲端運算的部署模型說明 [本研究整理]

	公用雲	私有雲	混合雲
服務範疇說明	1.不同的使用者是共享同一個業者所提供的雲端運算資料； 2.服務供應者把應用程式或儲存容量等雲端服務，經由網際網路提供給一般大眾	1.業者獨自建立與使用的雲端運算環境； 2.公司私有網路，利用虛擬化(Virtualization)和分散式計算(Distributed Computing)等雲端運算技術，以改善公司資源利用及降低管理開銷。	即為公有雲及私有雲之結合。使用者將不需要高資訊安全的資訊放到公有雲中，而將需要較高資訊安全的資訊放入使用者自行建立的私有雲中。
優點	企業可依需求向外訂購服務內容，無須考慮建置成本	資訊安全性高	兼顧公有雲及私有雲的優點，可簡化企業 IT 管理工作並降低整體維護成本
缺點	有安全疑慮	企業仍需花費大筆成本建置硬體環境，較不具彈性	公有雲與私有雲之間資料交換的機制須被克服
資訊安全性	低	高	居中
服務對象	外部客戶	內部客戶	兩者兼具

2.1.4 雲端運算分類

雲端運算分類定義如圖 3 所示，「服務消費者」透過雲端使用服務，「服務提供者」管 理雲端基礎架構，「服務開發者」則負責建 立服務 (注意：這些角色互動需要開放標準。)以下詳細說明每個角色的功能。

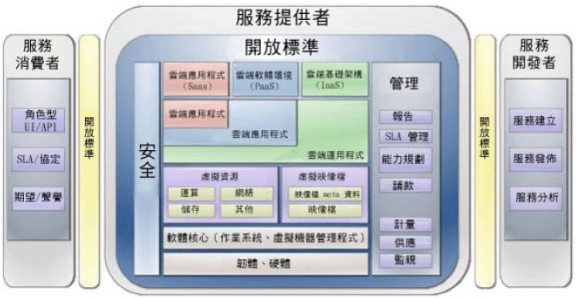

圖 3 雲端運算的分類

(1) 服務消費者：服務消費者為真正使用服務的使用者或企業，無論是「軟體」、「平台」、「基礎架構即服務」皆然。

根據服務類型及角色不同，消費者會運用不同使用者介面及程式介面，有些使用者介面外觀與其他應用程式無異，消費者使用應用程式時，不需瞭解雲端運算；其他使用者介面提供管理功能，如開關虛擬機器、管理雲端儲存空間等，消費者撰寫應用程式碼時，根據應用程式內容，使用 不同程式介面。

消費者也會接觸到服務層級協議(Service Level Agreement，SLA)[9]及其他協定，通常此部分會由消費者及供應者協商，消費者期望及供應者聲譽在協商過程中很重要。

(2) 服務供應者：服務供應者提供服務給消費者，實際項目則依服務種類有別：

(a) 「軟體即服務」而言，供應者安裝、管理及維護軟體，供應者不一定擁有軟體運作所需的實體基礎架構，消費者均無法接觸基礎架構，只能使用應用程式。

(b) 「平台即服務」而言，供應者為平台管理雲端基礎架構(通常為特定應用程式類型的基礎架構)，消費者的應用程式無法觸及平台背後基礎架構。

(c) 「基礎架構即服務」而言，供應者維護儲存空間、資料庫、訊息佇列或其他中介軟體，或是虛擬機器所在的主機環境，消費者使用時，將服務當成硬碟、資料庫、訊息佇列或機器，但無法觸及其管理基礎架構。

在服務供應者圖表中，最底層為基礎韌體及硬體，上一層則為軟體核心，為管理雲端基礎架構的作業系統或虛擬機器管理程式，虛擬資源與映像檔包括各種基本雲端運算服務，例如處理能力、儲存空間及中介軟體，由虛擬機器管理程式掌控的虛擬映像檔，包括映像檔本身及管 理所需的meta 資料。

管理層面對服務供應者的作業很重要，在基礎層次中，管理者需要一套計量方式，來決定使用者的身分及權限、安排資源給消費者、追蹤系統狀態

及資源。在較高層次中，管理工作包括攤平成本、確保可滿足消費者要求、SLA 管理(確保履行雙方協議內容)、通報高層等。

服務供應者運作須考量各層面的安 全(許多安全要求面向超出本報告討論範圍),也要符合開放標準，完善標準將簡化供應者運作內容，並確保與其他供應者的互通性。

(3) 服務開發者：

服務開發者建立、發佈及監控雲端服務，通常屬於「商務營運」應用程式，透過 SaaS 模式直接送至使用者手中，而在 IaaS 及 PaaS 層次撰寫的應用程式，也會受到 SaaS 開發者及雲端供應者採用。

建立服務的開發環境各有不同，若開發者在設計 SaaS 應用程式，很可能會為雲端供應者管理的環境撰寫程式碼，在這種情況下，發佈服務會將其部署在雲端供應者基礎架構中。在服務設計過程中，分析內容包括以遠端除錯作為測試，再發佈給消費者使用，服務一旦發佈後，分析數據能讓開發者監控服務效能，並進行必要修改。

(4) 雲端服務標準與分類關係:在每一種雲端服務(IaaS、PaaS、SaaS)中，開放標準能避免供應者套牢。

(a) 對 IaaS 而言,與雲端資 料庫合作的API若有標準，即可使用不同供應者的資料，共同 API 讓使用者可自由轉移至其他雲端資料庫供應者，但不需經過大幅變動，也會讓新資料來源與現有應用程式更容易整合。儲存、訊息佇列或 MapReduce 等其他雲端基礎架構的共同 API 亦有相似優點，資料與資料交換共同格式亦然。而在虛擬機器方面，共同虛擬機器格式非常重要，使用者應可取得由某雲端供應者建置及部署的虛擬機器，且不必做任何改變，即可將其部署至不同雲端供應者。

(b) 對 PaaS 而言，雲端提供的許多平台皆為應用程式基礎架構，這些基礎架構通常提供一般服務，如使用者介面、儲存與資料庫，但只能透過基礎架構下的 API 取用。

(c) 對 SaaS 而言，開放標準適用於應用程式層次，多數標準並非針對雲端運算，故這些標準不在本報告討論範圍內，例如雲端文書處理應用程式應支援文件可轉移性標準，這項要求與應用程式是否在雲端運作無關。

2.2 數位證據鑑識標準作業程序(DEFSOP)

數位鑑識(Digital Forensics)，又稱作電腦鑑識(Computer Forensics)，屬於鑑識科學的分支，用來取得數位物件中存有的數位化法律證據。數位鑑識的取證對象，從電腦系統、儲存媒體、電子文件檔案，至網路上傳輸的封包等均有。數位鑑識由於包含不同資訊專業領域，還可再細分為網路鑑識、資料庫鑑識與行動裝置鑑識等。

數位鑑識的應用範圍，除了最常見的法 律案件，用以釐清責任歸屬或舉證用，還可應用在故障系統的資料回復、分析系統入侵事件、蒐集數位證物，也能夠用來協助提升系統效能與除錯等。

所謂「數位鑑識」是從電腦中採集資訊作為證據的科學，用以解決網路犯罪難題的科學。數位鑑識，如同一般實物證據鑑識原則，對於數位證據的要求，應具「在不改變或破壞證物的情況下取得原始證物」、「證明所擷取的數位證據來自扣押的證物」、「在不改變證物的情況下進行分析」，亦即確保數位證據的完整性、正確性、一致性的前提下進行採證分析[9]。

參考國內學者林宜隆教授所提出數位證據鑑識標準作業程序(DEFSOP)[3]，如圖 4 所示[1]：

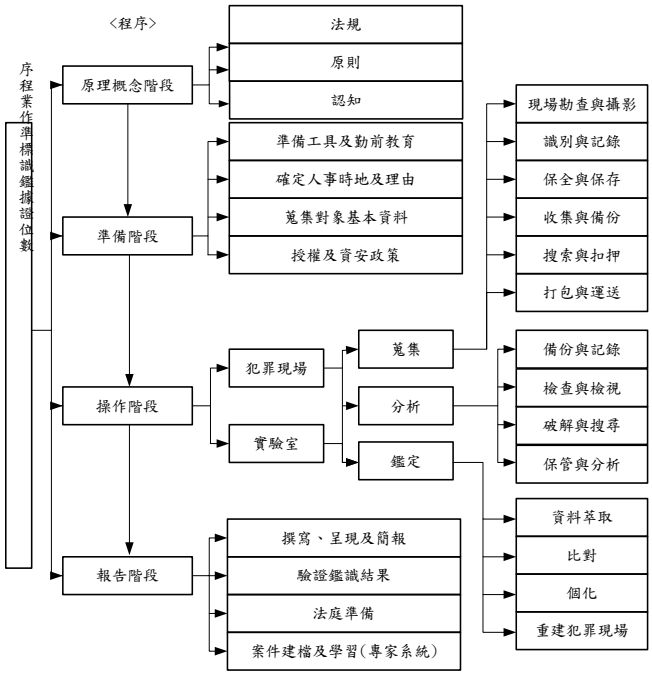

圖 4 數位證據鑑識標準作業程序(DEFSOP)

(1) 原理概念階段

(a) 法規：數位證據的取得要遵循合法、真實的原則，當事人不得以非法侵入他人電腦資訊系統的方法獲取證據；證據取得的途徑必須以立法的形式規定取得數位證據的程序及許可權。

(b) 原則：

- 完整性(Integrity)：在不改變或破壞證物的情況下取得原始證物。
- 正確性(Proper)：證明所擷取的數位證據來自扣押的證物。
- 一致性(Consistency)：在不改變證物的情況下進行分析。
- 符合性(Compliance)：符合當地的法律規範。

(c) 認知：對數位證據鑑識的意義與重要性

(2) 準備階段

本階段的主要工作是做一些鑑識前的準備工作，並蒐集相關資料，是為了操作階段各程序執行的預作準備，以下為其步驟：[4]

(a) 準備工具及勤前教育：必需準備電腦軟硬體規格的參考手冊、犯罪工具程式的參考手冊及破解電腦；在每次出任務前，必須計對鑑識人員進行進一步的說明，說明搜索任務、項目，並檢查軟硬體及工具是否準備齊全，以避免一些意外狀況發生。

(b) 確定人事時地及理由：根據犯罪的類型，並利用已掌握的情況分析可能作案人員，若案情需要也可訪談相關人員，另外再決定搜索地點、對象與時間，依據蒐集嫌犯資料後，決定搜索地點和時間。

(c) 蒐集對象基本資料：根據犯罪的類型，並利用已掌握的情況分析可能作案的人員，若案情需要也可訪談相關人員。

(d) 授權及資安政策：鑑識人員的授權並規劃鑑識執行的策略。

(3) 操作階段

(a) 蒐集程序：在蒐集資料這個程序，主要蒐集及採樣數位證據，將數位資料分為「變動性」、「固定性」、「檔案資料」三個部分。

(b) 分析程序：在分析資料這個程序，將分析資料分為五個部分，分別為「檔案」、「記錄檔(Log)」、「作業系統登入檔」、「判別惡意程式碼」、「其它(遠端主機通訊埠)」。

(c) 鑑定程序：在鑑定這個程序，將鑑定分為四個部分，分別為「資料萃取」、「比對」、「個化」、「重建犯罪現場」。

(4) 報告階段：在報告這個階段，將分為 4 個程序，分別為「撰寫、呈現及簡報」、「驗證鑑識結果」、「法庭準備」、「案件建檔及學習(專家系統)」。

3. 建立雲端安全數位證據鑑識標準作業程序雛型之探討

3.1 雲端安全風險之探討

雲端並未帶來任何新的安全威脅或問題，以安全而言，雲端運算整體是個理想使用案例，可彰顯無論雲端部署模型為何，安全基礎架構一致、透明與標準多麼重要。隨著企業轉移至雲端，或在雲端建立解決方案，擁有一致性安全模型儼然十分重要，除非如此做，才能簡化開發工作，並避免供應商套牢，節省企業資訊科技投資。

從雲端運算考量安全，最大差異在於企業失去掌控權，而非任何技術困難，在內部應用程式中，限制敏感資料及應用程式使用很重要，雲端應用程式存取控制同樣重要，但安全基礎架構、平台與應用程式直接受到雲端供應者掌控。以下是安全議題的次序：

(1) 法規：法規並非技術問題，但一定要處 理，法規所影響的安全要求凌駕於功能要求。

使用雲端運算時，除了所有技術問題，還有法規相關的殘酷現實。由於各種原因，世界各國政府均關切雲端運算使用問題，許多國家訂定嚴格隱私權法律，禁止特定資料儲存於國外實體機器中，組織或組織高層若違法將處重刑，任何組織若將敏感資料儲存於雲端，必須證明雲端供應者儲存資料時，並未存放在特定地區以外的實體伺服器內。

除政府機構之外，許多貿易及產業團體亦建立規範，這些規範或許無法律效力，但仍代表最佳範例。類似情況也發生在雲端運算的應用程式上，若虛擬機器在雲端上運作，在虛擬機器上運作的應用程式是否會接觸到敏感資料？這是個許多國家尚未觸及的灰色地帶，不過未來將會出現新法律與新規範。

(2) 安全管控：雖然消費者也許需要所有安全管控措施，但消費者仍需懷疑，雲端供應者基礎架構是否有能力提供所有安全相關保障。

適當管控是維護系統安全的必要條件，以下為「雲端運算使用案例白皮書」[8]中案例與管控要求之間關係如表 2 說明。

表 2 案例與管控要求之間關係說明

安全管控	內容說明
資產管理	必須能夠管理組成雲端基礎架構的所有硬體、網絡及軟體資產(實體與虛擬皆

	然)，包括對實體或網絡資產取用負責，並配合審核及監管。
加密：金鑰及憑證管理	任何安全系統都需要一套基礎架構，以 落實並管理加密金鑰與憑證，包括落實標準加密功能與服務，以支持靜止及 流通資訊安全。
資料/儲存安全	必須以加密格式儲存資料，此外，有些消費者資料儲存必須與其他消費者資料區隔。
終端安全	消費者必須能確保雲端資料終端安全，包括藉由網絡協定及設備種類限制終端。
事件審核與通報	消費者必須能得知雲端各項事件資料，尤其是系統錯誤與安全疏漏等，得知活動資訊包括瞭解歷史事件、通報新事件，雲端供應者若未及時通報事件，將嚴重損及聲譽。
身分、角色、存取控制與屬性	必須以一致、機器可讀的方式，定義身分、角色、權 利及其他個人及服務屬性，才能有效落實存取控制，並維護雲端資源安全政策。
網絡安全	必須在開關、路由器、封包等方面確保網絡流量安全，IP 程式本身也應安全。
安全政策	必須定義、解決與落實安全政策，以一致、機器可讀方式，支援存取控制、資源分配及其他決定，此種定義方法必須健全，才能讓 SLA 及授權自動生效。
服務自動化	必須以自動化方管理及分析安全管控流及程序，以支援安全監管審核，包括通報任何違反安全政策或客戶憑證協議的事件。
工作量及服務管理	必須依據安全政策及客戶憑證協議，以配置、部署及監控服務。

可應用於各項管控的部分標準如表 3 說明：

表 3 各項安全管控的相關標準說明

安全管控	相關標準
加密：金鑰及憑證管理	KMIP：OASIS「金鑰管理互通性協定」
資料/儲存安全	IEEE P1619：由 IEEE「儲存安全工作組」開發
身分、角色、存取控制與屬性	SAML：OASIS「安全判定標示語言」
	X.509 憑證：ITU「公開金鑰與屬性基礎架構建議」內容
安全政策	XACML：OASIS「可延伸存取控制標示語言」
工作量及服務管理	SPML：OASIS「服務供應標示語言」

(3) 安全聯合模式：為落實安全管控，需要不同的聯合模式，雲端供應者應透過現有安全標準提供聯合模式。

聯合亦即讓多項獨立資源如同單一資源運作，雲端運算本身即為聯合資源，故在單一雲端運算解決方案中，許多資產、身分、配置及其他細節必須聯合，才能發揮效果。要求透過以下聯合模式落實：

(a) 信任：指雙方在鑑別機構下建立信任關係的能力，鑑別機構能夠交換證明(通常為 X.509 憑證)，並以此確保訊息安全及建立已簽署的安全記號(通常為 SAML)，信任聯合是所有其他安全聯合模式的基礎。

(b) 身分管理：藉由使用者證明(帳號、密碼、文件)憑證身分，並回覆符合使用者的已簽署安全記號，服務提供者若信任身分提供者，縱然毫不認識使用者，亦可使用安全記號，開放適當權限給使用者。

(c) 使用管理：能夠制定政策(通常為 XACML)檢視安全記號，以管理雲端資源使用情況，使用資源會受到多個因素掌控，例如限制僅特定角色使用者可使用資源、只能在特定協定中使用、限制使用時段等。

(d) 單一登入/登出：根據可信任機構憑證匯整登入資訊，由於已鑑別使用者已具有特定角色，單一登入功能讓使用者只需登入某一應用程式，即可使用其他信任相同機構的其他應用程式。單一登出模式亦然，在許多情況下，使用者若自某一應用程式登出，就必須同時登出其他應用程式，單一登入模式需以身分管理模式為基礎才能執行。

(e) 審核及監管：可收集散佈在混合雲等多重網域內的審核及監管資料，聯合審核為必要工作，可確保並鑑活動符合 SLA 及法規要求。

(f) 配置管理：結合服務、應用程式及虛擬機器的配置資料，包括使用政策及跨網域授權資訊。

因為既有安全規範已應用在雲端運算，供應者應延用現有標準作為聯合模式。

3.2 雲端運算安全架構

雲端安全聯盟(CSA)建議進入雲端之前需要考慮的所有問題共有13個，這些問題可歸類為兩大類，即治理問題和運作問題[21]。在治理大項下，企業在評估雲端服務商時需要做風險管理評估，要問清楚存在哪些風險，誰來承擔風險，是雲端服務

商還是企業自己？法規遵從和審計擔保都有哪些？如何處理生命週期管理?在必要時如何提供電子證據？而在運作大項下，雲端服務商在提供業務連續性和災難恢復時能提供什麼樣的擔保？提供怎樣的資料加密？存取控制如何實行?諸如此類的問題都需要提給潛在的雲端服務商，並且需要在設計方案、服務合同以及服務等級協定中詳細落實。

雲端安全聯盟(CSA)針對雲端運算安全(Cloud Computing Security)提出了 12 個關注領域，並特別設法去解決雲端運算環境中的各種安全問題(如表 4 所示)，從而可應用於各種雲端服務和部署模式的結合。這些領域分成了兩大類：治理(Governance)和運作(Operating)。治理域範疇很寬，解決雲端運算環境的策略，而運作域則關注於安全考慮以及在架構內的實現運作。

表 4 CSA 的 12 個領域架構說明(本研究整理)

雲端運算架構框架Domain 1：Cloud Computing Architectural Framework	
治理域(Governance)	
域	指南解決的問題
治理和企業風險管理 Domain 2: Governance and Enterprise Risk Management	機構治理和評測雲端運算帶來的企業風險的能力。例如違約的司法慣例、用戶機構充分評估雲端提供商風險的能力、當用戶和提供商都有可能出現故障時保護敏感性資料的責任、國際邊界對這些問題有何影響等都是討論的一些問題。
法律和電子證據發現 Domain 3: Legal and Electronic Discovery	使用雲端運算時可能的法律問題。本部分關係到的問題包括資訊和電腦系統的保護要求、安全性被破壞時的披露法律、監管要求、隱私要求和國際法等。
合規性和審計 Domain 4: Compliance and Audit	這部分考慮保持和證實使用雲端運算時的合規性，包括評估雲端運算如何影響內部安全性原則的合規性、以及不同的合規性要求(規章、法規等)。這個域還包括通過審計證明合規性的一些指導。
資訊生命週期管理 Domain 5: Information Lifecycle Management	以下這些問題將在這部分討論：管理雲端的資料，包括與身份和雲端的資料控制相關的項;可用於處理資料搬移到雲端時失去物理控制這一問題的補償控制；其它項，如誰負責資料機密性、完整性和可用性等
可攜性和互通性 Domain 6: Portability and Interoperability	將資料或服務從一個提供商搬移到另一個提供商，或將它全部搬移到本地的能力。提供商間互通性相關的問題也在這裡討論。
運作域(Operating)	
域	指南解決的問題
傳統安全、業務連續性和災難恢復 Domain 7: Traditional Security, Business Continuity, and Disaster Recovery	雲端運算如何影響當前用於實現安全性、業務連續性和災難恢復的操作處理和規程，主要關注點是討論和檢查雲端運算的潛在風險，希望增加對話和討論以解決令人生畏的企業風險管理模型的提升需求。進而，本節還討論了如何幫助人們識別雲端運算在什麼地方可以有助於減少安全風險，在某些其它領域則增加了風險。
資料中心運行 Domain 8: Data Center Operations	如何評估提供商的資料中心架構和運行。主要關注在說明使用者識別對於後面服務不利的資料中心特徵，以及有助於長期穩定性的基礎特徵。
事件回應、通告和補救 Domain 9: Incident Response, Notification, and Remediation	適當的、充分的事件檢測、響應、通告和補救。嘗試解決為了啟動適當的事件處理和事後分析機制，在用戶和提供商兩邊都需要就緒的一些條目。本域將會幫助您理解雲端給您現有的事件處理常式帶來的複雜性。
應用安全 Domain 10: Application Security	保護在雲端運作或即將開發的應用。包括將某個應用遷移到或設計進雲端運作是否適當，如果適當，什麼類型的雲端平台最適當(SaaS, PaaS, or IaaS)。還討論了一些跟雲端有關的具體安全問題。
加密和金鑰管理 Domain 11: Encryption and Key Management	識別恰當使用加密以及可擴充規模的金鑰管理的方法。本節並不是什麼規定，而是側重提供資訊，為什麼需要這些方法，識別使用過程中出現的問題，包括保護對資源的存取以及保護資料。
身份和存取管理 Domain 12: Identity and Access Management	利用目錄服務來管理身份，提供存取控制能力。關注點是組織將身份管理擴展進雲端遇到的問題。本域提供了就評估組織實施身份存取管理IAM的就緒性的一些見解。
虛擬化 Domain 13: Virtualization	虛擬化在雲端運算中的應用。本領域關係到與多租戶、VM 隔離、VM共居(coresidence)、hypervisor脆弱性等相關的項。特別關注於系統和硬體虛擬化相關的安全問題，而不是對各種形式的虛擬化的綜述。

雲端安全聯盟(CSA)報告提出了雲端運算帶來的最大的七項風險，並提出相關補救建議[6]、[10]，該報告由「雲端安全聯盟」和「惠普公司」合作完

成。這七項風險分別是(如表 5 所示)：

- 風險 1：濫用和惡意使用雲端運算

IaaS(基礎架構即服務)雲端運算服務商為客戶提供了無限的計算、網路、存儲資源，客戶只要擁有信用卡就可以註冊使用，有的服務商甚至為使用者提供了免費試用期。但是這種便利性可能被垃圾郵件、惡意軟體或其他網路罪犯所利用。PaaS(平台即服務)曾飽受此苦。

- 風險 2：不安全的應用程式介面(API)

雲端運算提供商為客戶提供了一系列軟體介面和 API，以說明他們管理和使用雲端運算服務。雲服務的安全性與可獲得性依賴於 API 的安全性，比如身份驗證、存取控制、加密、用戶活動監測等。此外，通常還有協力廠商機構以這些 API 為基礎為其使用者提供增值服務，這就增加了 API 的複雜度和風險。

- 風險 3：內部破壞

來自於服務商內部的惡意行為是一個眾所周知的問題。但在單一管理機制下，雲端運算服務商的操作機制缺乏透明度，因而來自於雲端運算服務商內部的惡意行為對於用戶來說會更為嚴重。例如，服務商不會公開是按照什麼機制向其雇員授予物理資產和虛擬資產的存取權限，以及如何監控其雇員的行為。這種情況為駭客行為、有組織的犯罪、間諜活動等提供了便利，導致機密資料被盜或整個雲服務被控制。

- 風險 4：共用技術問題

IaaS 服務商為使用者提供可共用的基礎架構，並採用了虛擬化管理程式作為使用者作業系統和物理資源之間的媒介。但這些虛擬化管理程式存在缺陷，使用者作業系統有可能會控制或影響底層平台，因而用戶的操作可能影響其他用戶的操作。

- 風險 5：資料丟失或洩漏

導致資料丟失的原因包括在未備份的情況下進行資料刪除和修改、將資料存儲在不可靠的介質上等。允許未授權使用者訪問敏感性資料則可能導致資料洩漏。

- 風險 6：帳戶或服務綁架

通過網路釣魚、詐騙、軟體漏洞等可以實現帳戶或服務綁架，即使用者的身份和密碼資訊被攻擊者掌握。如果使用者信用卡資訊被盜取，則攻擊者就能夠利用用戶的身份開展一系列攻擊。

- 風險 7：未知的風險

雲端運算的一項宗旨就是減輕軟硬體的管理任務，讓用戶集中精力發揮核心優勢，但也會在升級、資訊共用等過程中帶來一些未知的風險。

表 5 Top Threats to Cloud Computing [本研究整理]

項次	風險	補救建議	雲運算關鍵領域安全指南參考	服務類型
1	濫用和惡意使用雲端運算	1.執行更嚴格的註冊和驗證措施； 2.加強信用卡詐騙監測與協作； 3.全面監測使用者網路流量； 4.監測公共黑名單。	D8：資料中心運行 D9：應急回應、通告和補救	IaaS PaaS
2	不安全的介面和APIs	1.分析雲服務商API介面的安全模式； 2.確保對加密傳輸實行嚴格的身份驗證和存取控制； 3. 認識與API相關的依賴鏈(dependency chain)。	D10：應用安全	IaaS PaaS SaaS
3	惡意的內部人員	1.執行嚴格的供應鏈管理,對供應商進行全面的評估； 2.在合同中對人力資源提出詳細要求; 3.要求保證資訊安全、管理實踐和一致性報告的透明度； 4.制定安全破壞通知程式。	D2：治理和企業風險管理 D7：傳統安全、業務連續性和災難恢復	IaaS PaaS SaaS
4	共用技術問題	1.執行安裝/配置的最佳安全實踐； 2.監測非授權變化/活動的環境； 3.對管理許可權與操作執行嚴格的身份認證與存取控制； 4.對於補丁和漏洞修補執行服務等級協定； 5.執行漏洞掃描和配置審計。	D8：資料中心運行 D13：虛擬化	IaaS

5	資料丟失或洩漏	1.執行嚴格的API存取控制； 2.資料傳輸時對資料加密並保持其完整性； 3.在設計階段和運行時分析對資料的保護情況； 4.執行嚴格的金鑰生成、存儲、管理與銷毀實踐； 5.在合同中要求雲服務商在把存儲介質放回資源池前要徹底清除使用者資料； 6.在合同中詳細規定雲服務商的備份與保留策略。	D5：資訊生命週期管理 D11：加密和金鑰管理 D12：身份和訪問管理	IaaS PaaS SaaS
6	帳戶或服務綁架	1.禁止共用使用者和服務的帳戶證書; 2.盡可能使用嚴格的雙重身份驗證技術； 3.對非授權活動進行主動監測； 4.學習雲服務商的安全政策和服務等級協定。	D2：治理和企業風險管理 D9：應急回應、通告和補救 D12：身份和訪問管理	IaaS PaaS SaaS
7	未知的風險	1.公開應用日誌和資料； 2.部分/完全公開基礎設施詳細資訊； 3.監測必要資訊。	D2：治理和企業風險管理 D3：法律和電子證據發現 D8：資料中心運行 D9：應急回應、通告和補救	IaaS PaaS SaaS

3.3 雲端安全聯盟控制模型(CSA Controls Matrix)

雲端安全聯盟(CSA)[23]制定了一套叫做雲端控制模型(Cloud Controls Matrix，CM)的基本安全規則[12]，開發出一套針對雲端服務進行安全性評估的公開問題集，共有 11 大項安全規則控制區；98 項安全規則控制 ID，說明如下[13][14]：

(1) 規範(Compliance，CO-01~06)：審計計畫(CO-01)、獨立計畫(CO-02)、第三方審計(CO-03)、聯繫/授權維護(CO-04)、資訊系統控制對映(CO-05)、智慧財產(CO-06)

(2) 資料治理(Data Governance ，DG-01~08)：所有權/管理職責(DG-01)、分類(DG-02)、處理/標記/安全政策(DG-03)、保留政策(DG-04)、安全處置(DG-05)、非生產資料(DG-06)、資訊洩漏(DG-07)、風險評估(DG-08)

(3) 設施安全(Facility Security ，FS-01~08)：政策(FS-01)、使用者存取(FS-02)、控制存取點(FS-03)、安全區域授權(FS-04)、未經授權的人士進入(FS-05)、非現場授權(FS-06)、非現場設備(FS-07)、資產管理(FS-08)

(4) 人力資源(Human Resources，HR-01~03)：背景審查(HR-01)、僱用協議(HR-02)、僱用終止(HR-03)

(5) 資訊安全(Information Security，IS-01~34)：管理計畫(IS-01)、管理支持/參與(IS-02)、政策(IS-03)、需求底限(IS-04)、政策複審(IS-05)、政策執行(IS-06)、使用者存取政策(IS-07)、使用者存取限制/授權(IS-08)、使用者存取廢止(IS-09)、使用者存取複審(IS-10)、培訓/認知(IS-11)、企業知識/基準評價(IS-12)、角色/職責(IS-13)、管理監督(IS-14)、權責劃分(IS-15)、使用者責任(IS-16)、工作區(IS-17)、加密(IS-18)、加密密鑰管理(IS-19)、漏洞/修補管理(IS-20)、反病毒/惡意軟體(IS-21)、事件管理(IS-22)、事件報告(IS-23)、事件反應法律預備(IS-24)、事件反應衡量(IS-25)、可接受的使用(IS-26)、資產報酬率(IS-27)、電子商務交易(IS-28)、審計工具存取(IS-29)、特徵的/配置埠存取(IS-30)、網路/基礎架構服務(IS-31)、便攜式/移動設備(IS-32)、原始碼存取限制(IS-33)、應用程序存取(IS-34)

(6) 法律(Legal ，LG-01~02)：非公開協議(LG-01)、第三方協議(LG-02)

(7) 操作管理(Operations Management，OP-01~04)：政策(OP-01)、文件(OP-02)、容量/資源規劃(OP-03)、設備維護(OP-04)

(8) 風險管理(Risk Management，RI-01~05)：程式(RI-01)、評估(RI-02)、減輕/接受(RI-03)、商業/政策變化影響(RI-04)、第三方存取(RI-05)

(9) 發佈管理(Release Management，RM-01~05)：新開發/獲得(RM-01)、生產變動(RM-02)、品質檢測(RM-03)、外包開發(RM-04)、未經授權的軟體安裝(RM-05)

(10) 恢復能力(Resiliency，RS-01~08)：管理程序(RS-01)、影響分析(RS-02)、業務持續規劃(RS-03)、業務持續測試(RS-04)、環境風險(RS-05)、設備位置(RS-06)、設備電源故障

(RS-07)、電力/電信(RS-08)

(11) 安全架構(Security Architecture ，SA-01~15)：客戶存取需求(SA-01)、使用者的 ID 憑證(SA-02)、資料完全/完整性(SA-03)、應用安全(SA-04)、資料完整性(SA-05)、生產/非生產環境(SA-06)、遠端使用者多因素驗證(SA-07)、網路安全(SA-08)、分割(SA-09)、無線網路安全(SA-10)、共享網路(SA-11)、時鐘源同步(SA-12)、設備識別(SA-13)、審計日誌/入侵檢測(SA-14)、移動代碼(SA-15)

3.4 雲端安全數位證據鑑識標準作業程序(CCS-DEFSOP)雛型之探討

整理雲端安全聯盟(CSA)與歐盟(ENISA)報告中所提出之安全風險問題整理比較，發現共有 4 個安全風險問題相似(不安全的 API 介面/管理界面妥協、內部破壞/惡意的內部人士、共用技術問題/隔離失敗、資料丟失或洩漏/資料保護/不安全或不完整的資料刪除)，合計 9 個安全風險問題，如表 6 說明：

表 6 CSA/ENISA for Risks 與 CSA Domain 對映說明表

項次	安全風險	說明內容	CSA 指南參考	備註
1	濫用和惡意使用雲端運算 Abuse and Nefarious Use of Cloud Computing	IaaS(基礎架構即服務)雲端運算服務商為客戶提供了無限的計算、網路、存儲資源，客戶只要擁有信用卡就可以註冊使用，有的服務商甚至為使用者提供了免費試用期。但是這種便利性可能被垃圾郵件、惡意軟體或其他網路罪犯所利用。PaaS(平台即服務)曾飽受此苦。	D8：資料中心運行 D9：應急回應、通告和補救	CSA
2	不安全的介面和 APIs Insecure Interface and APIs/管理界面妥協 Management Interface Compromise	雲端運算提供商為客戶提供了一系列軟體介面和 API，以說明他們管理和使用雲端運算服務。雲服務的安全性與可獲得性依賴於 API 的安全性，比如身份驗證、存取控制、加密、用戶活動監測等。此外,通常還有協力廠商機構以這些 API 為基礎為其使用者提供增值服務，這就增加了 API 的複雜度和風險。	D10：應用安全	CSA ENISA
3	惡意的內部人員 Malicious Insiders/惡意的內部人士 Malicious Insider	來自於服務商內部的惡意行為是一個眾所周知的問題。但在單一管理機制下，雲端運算服務商的操作機制缺乏透明度，因而來自於雲端運算服務商內部的惡意行為對於用戶來說會更為嚴重。例如，服務商不會公開是按照什麼機制向其雇員授予物理資產和虛擬資產的存取權限，以及如何監控其雇員的行為。這種情況為駭客行為、有組織的犯罪、間諜活動等提供了便利，導致機密資料被盜或整個雲服務被控制。	D2：治理和企業風險管理 D7：傳統安全、業務連續性和災難恢復	CSA ENISA
4	共用技術問題 Share Technology Issues/隔離失敗 Isolation Failure	IaaS 服務商為使用者提供可共用的基礎架構，並採用了虛擬化管理程式作為使用者作業系統和物理資源之間的媒介。但這些虛擬化管理程式存在缺陷，使用者作業系統有可能會控制或影響底層平台，因而用戶的操作可能影響其他用戶的操作。	D8：資料中心運行 D13：虛擬化	CSA ENISA
5	資料丟失或洩漏 Data Loss or Leakage/資料保護 Data Protection/不安全或不完整的資料刪除 Insecure or Incomplete Data	導致資料丟失的原因包括在未備份的情況下進行資料刪除和修改、將資料存儲在不可靠的介質上等。允許未授權使用者訪問敏感性資料則可能導致資料洩漏。	D5：資訊生命週期管理 D11：加密和金鑰管理 D12：身份和存取管理	CSA ENISA

	Deletion			
6	帳戶或服務綁架 Account or Service Hijacking	通過網路釣魚、詐騙、軟體漏洞等可以實現帳戶或服務綁架，即使用者的身份和密碼資訊被攻擊者掌握。如果使用者信用卡資訊被盜取，則攻擊者就能夠利用用戶的身份開展一系列攻擊。	D2：治理和企業風險管理 D9：應急回應、通告和補救 D12：身份和存取管理	CSA
7	管理的損失 Loss Of Governance	在使用雲基礎架構的過程中，客戶把影響安全的控制權問題轉移給雲端供應者(Cloud Provider，CP)。同時，SLAs 可能不會有提供這樣雲端服務的承諾，因此在安全防禦留下給一個缺口。	D2：治理和企業風險管理	ENISA
8	閉鎖性 Lock-In	目前很少有提供工具、程序、標準資料格式或者服務介面的方法可以保證資料、應用程序和服務的可攜性。使用者從一個供應者轉移到另一個供應者，或者轉移資料和服務到內部的 IT 環境是困難。這說明了依賴特定的 CP 者的服務提供，特別是把資料可攜性作當是基本面向是不可行的。	D6：可攜性和互通性	ENISA
9	規範風險 Compliance Risks	在取得認證方面(例如，企業標準或者法規要求)的投資可能受到風險，在轉移到雲端運算環境。 1.如果 CP 不能提供他們自己規範的相關要求證據。 2.如果 CP 不允許被雲端用戶審核。 在某些情況裡，也表明使用公眾雲端基礎架構上某些規範的種類是不可能實現(例如，PCI DSS[16])。	D4：合規性和審計	ENISA

參考雲端安全聯盟所提出的 12 個雲端安全的關注領域，對應林宜隆教授的 PLSE Model 的四個面向(政策面、法律面、技術面、教育面)，如圖 5 說明；並探討 CSA 報告「CSA Control Matrix」的基本安全規則，對雲端服務進行安全性評估問題規範，如圖 6 說明。

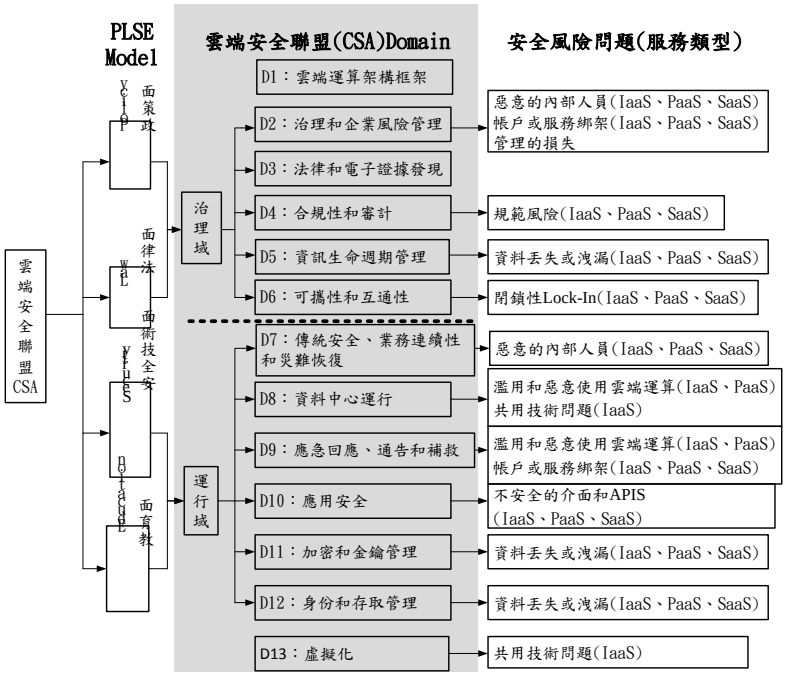

圖 5 CSA Domain for Risks 與 PLSE 模型對映說明

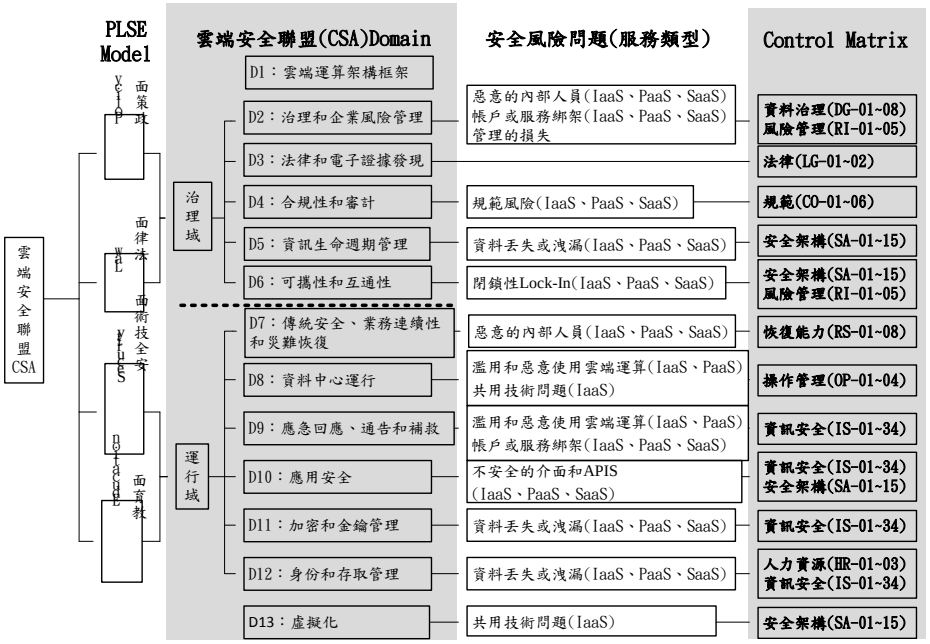

圖 6 CSA Domain Risks 與 Control Matrix 對映圖 (含 PLSE 模型)

參考國內學者林宜隆教授所提出數位證據鑑識標準作業程序(DEFSOP)並探討 CSA Control Matrix 的基本安全規則，對雲端服務進行安全性評估問題能與數位鑑識標準作業程序對映並應用，進而提出於雲端安全之數位證據鑑識標準作業程序(CCS-DEFSOP)。數位證據鑑識標準作業程序(DEFSOP)與 CSA Control Matrix 報告的規範互相對映遵循說明(如圖 7、圖 8、圖 9、表 7 說明)：

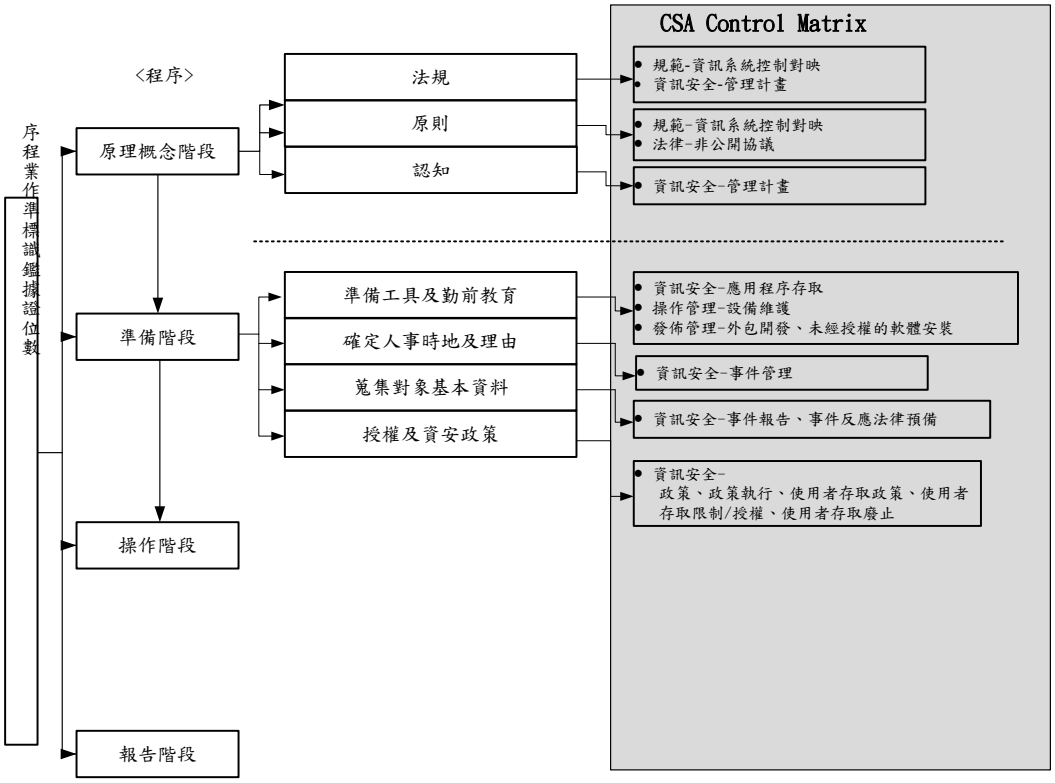

圖 7 DEFSOP 與 Control Matrix 對映圖(原理概念、準備階段)

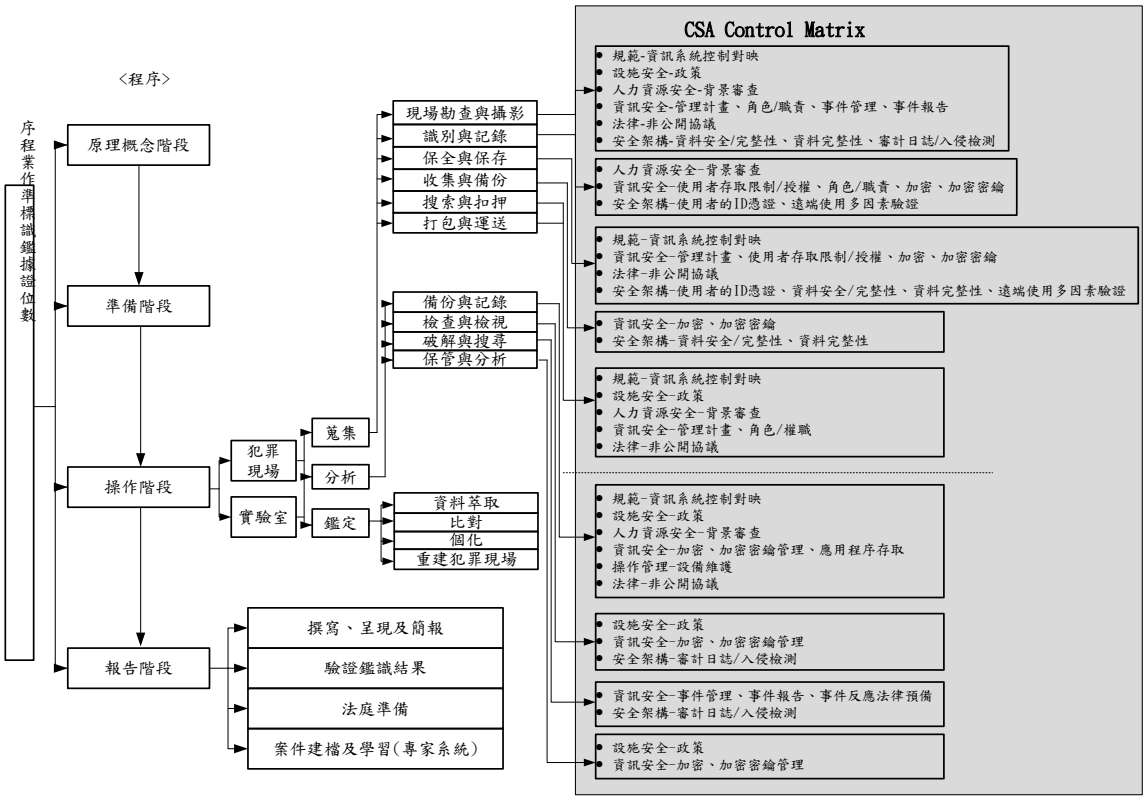

圖 8 DEFSOP 與 Control Matrix 對映圖(操作階段-蒐集、分析程序)

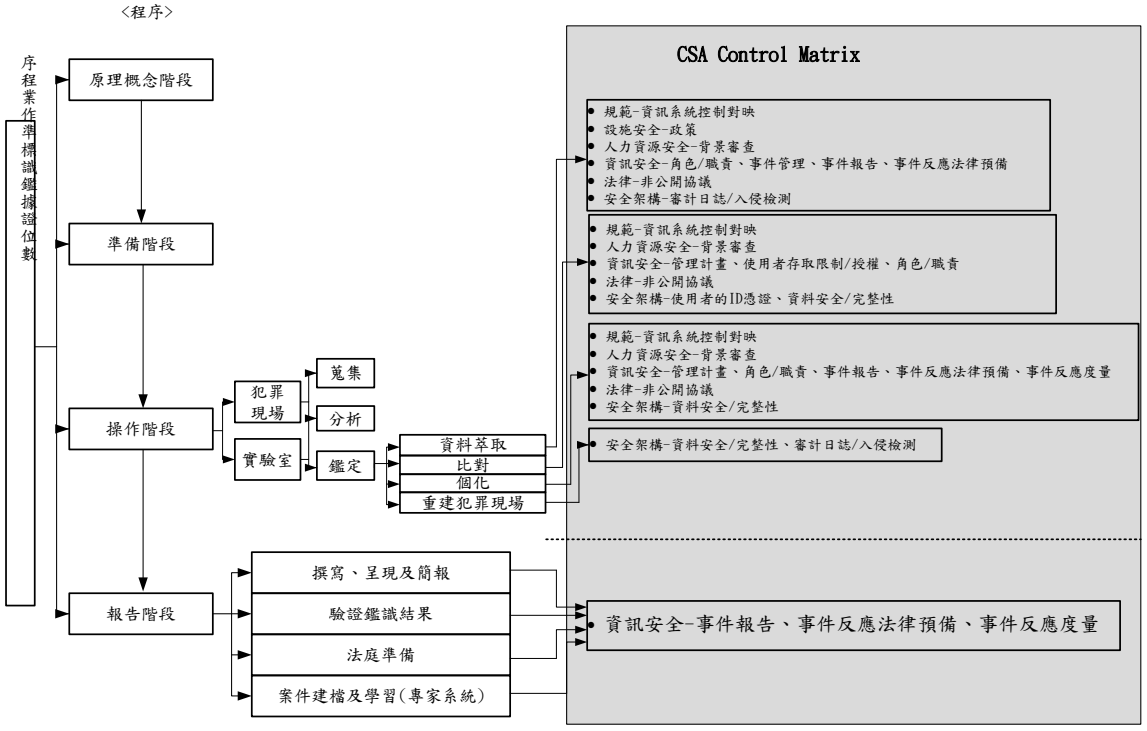

圖 9 DEFSOP 與 Control Matrix 對映圖(操作階段-鑑定程序、報告階段)

表 7 DEFSOP 與 CSA Controls Matrix(CM)項目對映說明

DEFSOP 四階段	四階段的項目	CSA Controls Matrix(CM)-Control ID	說明
原理概念階段	原則	Compliance：CO-05 Information Security：IS-01	數位證據鑑識的目標與標準。
	法規	Compliance：CO-05 Legal：LG-01	數位證據鑑識於法規中所具

			備的證據力與證明力。
	認知	Information Security：IS-01	數位證據鑑識的意義與重要性。
準備階段	準備工具資料及勤教	Information Security：IS-34 Operations Management：OP-04 Release Management：RM-04、05	準備蒐集、分析及鑑識所需工具軟體。
	確定人事時地及理由	Information Security：IS-22	確認鑑識環境與各項環境資料。
	蒐集對象基本資料	Information Security：IS-23、24	蒐集檢視鑑識目標的資料。
	授權及資安政策	Information Security：IS-03、06、07、08、09	鑑識所需環境與法規流程。
操作階段	蒐集	Information Security：IS-24	蒐集及採樣數位證據。
	蒐集-現場勘查與攝影	Compliance：CO-05 Information Security：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行勘查於攝影。
		Human Resources Security：HR-01 Information Security：IS-13	識別現場環境與任務執行人員身分。
		Facility Security：FS-01	測試設備及監督現場執行狀況。
		Information Security：IS-22、23 Security Architecture：SA-14	勘查現場執行狀況的安全事件定義。
		Security Architecture：SA-03、05	攝影及現場勘查資訊的保存與傳輸交換。
	蒐集-識別與記錄	Human Resources Security：HR-01 Information Security：IS-13	人員身分的識別，勤務人員的管制與記
			錄。
		Security Architecture：SA-02、07 Information Security：IS-08	管理人員登入與執行鑑識時的帳號。
		Information Security：IS-18、19	人員身分登入及使用記錄均需採取加密保護。
			身分及文件的密碼管理。
	蒐集-保全與保存	Compliance：CO-05 Information Security：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行保全與保存。
		Security Architecture：SA-02、07 Information Security：IS-08	管理人員登入與執行鑑識時的帳號。
		Information Security：IS-18、19	人員身分登入及使用記錄均需採取加密保護。
			身分及文件的密碼管理。
		Security Architecture：SA-03、05	資訊的保存與傳輸交換。
	蒐集-收集與備份	Information Security：IS-18、19	人員身分登入及使用記錄均需採取加密保護。
			身分及文件的密碼管理。
		Security Architecture：SA-03、05	資訊的保存與傳輸交換。
	蒐集-搜索與扣押	Compliance：CO-05 Information Security：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行搜索與扣押。
		Human Resources Security：HR-01	人員身分的識別，勤

		Information Security：IS-13	務人員的管制與記錄。
		Facility Security：FS-01	測試設備及監督現場執行狀況。
	蒐集-打包與運送	Compliance：CO-05 Information Security：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行打包與運送。
		Human Resources Security：HR-01 Information Security：IS-13	人員身分的識別，勤務人員的管制與記錄。
		Facility Security：FS-01	測試設備及監督現場執行狀況。
	分析	Information Security：IS-34 Operations Management：OP-04	1. 分析數位證據的資料。 2. 運用軟體與工具分析所蒐集及採樣的證據。
	分析-備份與記錄	Compliance：CO-05 Information Security：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行備份與記錄。
		Human Resources Security：HR-01 Information Security：IS-13	人員身分的識別，勤務人員的管制與記錄。
		Information Security：IS-18、19	人員身分登入及使用記錄均需採取加密保護。
	分析-檢查與檢視	Facility Security：FS-01	測試設備及監督現場執行狀況。
		Information Security：IS-18、19	人員身分登入及使用記錄均需採取加密保護。
			檢查與檢視數位證據中惡意程式的活動，須保留不予移除(還原犯罪證據)。
	分析-破解與搜尋	Information Security：IS-22、23、24 Security Architecture：SA-14	安全測試犯罪證據的破解與搜尋，並完整監督與記錄過程。
			於破解與搜尋後亦須定義其犯罪事件的區分。
			檢查與檢視數位證據中惡意程式的活動，須保留不予移除(還原犯罪證據)。
			破解與搜尋過程中需記錄與偵測網路的活動。
	分析-保管與分析	Facility Security：FS-01	測試設備及監督現場執行狀況。
		Information Security：IS-18、19	人員身分登入及使用記錄均需採取加密保護。
	鑑定	Security Architecture：SA-14	鑑定證據所具備的證據力與證明力。
	鑑定-資料萃取	Compliance：CO-05 Information Security：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行資料萃取。
		Human Resources	人員身分

		Security：HR-01 Information Security ：IS-13	的識別，勤務人員的管制與記錄。
		Facility Security：FS-01	測試設備及監督現場執行狀況。
		Information Security ：IS-22、23、24	於資料萃取後亦須定義其犯罪事件的區分與證明力。
			分析所萃取的惡意活動資料，並預防其自動刪除的問題。
			分析網路活動並萃取其資料。
	鑑定-比對	Compliance：CO-05 Information Security ：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行比對。
		Human Resources Security：HR-01 Information Security ：IS-13	人員身分的識別，勤務人員的管制與記錄。
		Information Security ：IS-08 Security Architecture：SA-02	進行比對程序時，需進一步管理使用者的權限。
		Security Architecture：SA-03	於比對程序時，需測試數位證據的安全性，並記錄與監督過程符合數位證據的保存。
			比對與分析過程均需預防惡意軟件的自動移除。
			比對時確

			保網路的活動與環境，以利還原犯罪證據。
	鑑定-個化	Compliance：CO-05 Information Security ：IS-01 Legal：LG-01	依據所頒定標準作業程序及法規執行個化。
		Human Resources Security：HR-01 Information Security ：IS-13	人員身分的識別，勤務人員的管制與記錄。
			個化犯罪事件資料需通過安全測試，並監督其過程。
		Security Architecture：SA-03	定義個化犯罪事件資料的安全區分。
		Information Security ：IS-25	個化區分惡意軟件的特徵並列出偵測與預防的方式。
		Information Security ：IS-23、24	藉由個化，定義此事件或證據所具備的網路條件。
	鑑定-重建犯罪現場	Security Architecture：SA-03、14	安全測試與監督所還原的數位證據。
			定義與區分所重建的犯罪證據。
			安全保護所還原的犯罪證據。
			偵測所還原的惡意軟件活動。
			重建犯罪證據的網

			路環境與條件。
報告階段	撰寫、呈現及簡報 案件建檔及學習	Information Security：IS-23、24、25	按照法規程序，呈現及撰寫鑑識結果報告。
	驗證鑑識結果		比對證據與驗證報告。
	法庭準備		呈現報告所具備的公信力。
	案件建檔及學習		案件儲存及列入勤教教材。

4. 結論與建議

本研究的目的為透過雲端運算架構、應用及安全威脅議題進行探討，並針對雲端安全聯盟(CSA)所提出的 12 個雲端安全的關注領域，對應林宜隆教授的提出 PLSE Model(Policy、Law、Security、Education)模型的四個面向(政策面、法律面、安全技術面、教育面)，探討 CSA Control Matrix 的基本安全規則，對雲端服務進行風險安全性評估問題之探討。

研究探討雲端服務進行安全性風險評估規範能與數位鑑識標準作業程序對映並應用，進而提出於雲端安全之數位證據鑑識標準作業程序(CCS-DEFSOP)，進一步可提供已導入或通過 ISO/IEC 27001 企業組織及政府機關面對未來雲端運算環境之安全服務評估參考資料或檢查項目(Checklist)。

參考文獻

[1] 宜隆、藍添興，2004年，資訊犯罪與安全管理之探討，中央警察大學

[2] 林宜隆、朱惠中、張志欶，2008年，「數位證據鑑識標準作業程序與案例驗證之建構—以Windows XP系統為例」，華梵大學，2008數位科技與創新管理研討會。

[3] 林宜隆、朱惠中、吳穩男與張志欶等，2008年，「數位證據鑑識標準作業程序與案例驗證之建構-以Linux/Unix系統為例」，輔仁大學，2008聯合國際研討會。

[4] 林宜隆，2009年，「網路犯罪理論與實務」，中央警察大學出版社，頁607~608。

[5] 柯宏叡、王旭正、黃嘉宏、詹前隆，2007年，「資訊戰攻擊與入侵證據鑑識」，資通安全專論T96010。

[6] 唐川 編譯，2010年，「研究報告列舉雲運算七大風險」，信息化研究與應用快報，第7期，頁9~12。

[7] 歐陽惠華、楊中皇、樊國楨，2007年，「ISO 27002與COBIT 4.1控制措施之對映分析」，碩士論文，高雄師範大學。

[8] 雲端運算使用案例白皮書，第三版，2010年，Cloud Computing Use Cases group，http://www.cloudusecases.org/

[9] Balachandra Reddy Kandukuri and Ramakrishna Paturi V(2009)," Cloud Security Issues" ,IEEE.

[10] Cloud Security Alliance(2010)，" Security Guidance for Critical Areas of Focus in Cloud Computing V2.1"，(http://www.cloudsecurityalliance.org/guidance/)

[11] Cloud Security Alliance(2010)，"Top Threats to Cloud Computing V1"(http://www.cloudsecurityalliance.org/topthreats.html)

[12] Cloud Security Alliance(2010)，" CSA Cloud Controls Matrix V1 is Released"，(http://www.cloudsecurityalliance.org/cm.html)

[13] Control Objectives for Information and related Technology (COBIT®), Version 4.1 (2007)，http://www.isaca.org

[14] International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27002:2005 -- Information technology -- Security techniques -- Code of practice for Information Security Management，http://www.iso.org/iso/iso_catalogue.htm

[15] NIST，http://csrc.nist.gov/groups/SNS/cloud-computin

[16] PCI Security Standards Council [Online] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

[17] Warren G. Kruse and Jay G. Heiser(2002)，" Computer Forensics: Incident Response Essentials" ，ddison-Wesley Pearson Higher Education.

[18] 中華徵信/專題剖析，李奕欣，企業雲端服務建置需求，http://www.credit.com.tw/CreditOnline/cfcontent/Market/weekly/index.cfm?sn=70

[19] 台彎電腦網路危機處理暨協調中心技術專欄，電腦鑑識科學的現在與未來(一)，http://www.cert.org.tw/document/column/

[20] e化部落，林育竹，雲端運算 Cloud Computing 的概念與應用，http://eblog.cisanet.org.tw/post/Cloud-Computing.aspx

[21] e NET/IT運維，企業進入雲兩類問題：營運+治理問題，

http://www.enet.com.cn/article/2010/0827/A20100827715200.shtml
[22] IT部落格，[Cloud Computing]三種雲端服務，http://www.dotblogs.com.tw/jimmyyu/archive/2009/12/03/12275.aspx
[23] Cloud Security Alliance，http://www.cloudsecurityalliance.org/