國軍雲端資料中心資訊安全評估指標之研究

蘇品長[1]　劉定衢[1]　王振漢[2]　羅文榮[2*]

[1]國防大學管理學院資訊管理學系

[2]國防部後備指揮部

論文編號：4102-1
來稿2020年3月25日→第一次修訂2021年7月19日→同意刊登2021年8月16日

摘要

隨著網際網路發展與普及，敵人可透過網路癱瘓軍事或民生基礎設施，網路攻擊已成為軍事攻擊手段的一種。國防部遵循行政院資訊機房共構及節能減碳政策，現正於軍網規劃適用於國軍之雲端資料中心，收容資訊服務，統一調度資訊資源，以滿足各級資訊作業需求。然而，集中資源本身就是一種風險，故如何評估及落實雲端資料中心資訊安全作為，防止國防秘密被竊取或基礎設施遭破壞，已成為重要課題。本研究結果發現，主要構面權重以「組織與人員專業能力」最高，在第三層細部指標權重值，以「高階主管資訊安全認知與支持」、「人員安全考核」及「系統操作及管理能力」等三項最為重要。故就整體而言，國軍在建構專屬雲端資料中心時，「人」對於資訊安全的影響，要重於「設備」與「管理」；因此，提升高階主管資訊安全素養，落實考核及評估資訊人員適任性，以及透過人員訓練使開發之系統符合資安防護規範，均屬當務之急。

關鍵詞：雲端資料中心、資訊安全指標、德爾菲法、層級分析法

[*] 聯絡作者：羅文榮 email:：lewensin@gmail.com

A Study of Information Security Evaluation Indicators for Military Cloud Data Center

Su, Pin-Chang [1] Liu, Ding-Chyu [1] Wang, Jen-Hang [2] Lou, Wen-Long [2*]

[1] Department of Information Management, National Defense University, Taiwan, R.O.C.
[2] Armed Force Reserve Command , Taiwan, R.O.C.

Abstract

Due to the development and popularity of the Internet, hostile countries can destroy military or civilian infrastructure through the Internet. Cyber-attacks have become a form of military attack today. The Ministry of National Defense (MND) follows the policy of information equipment co-location and energy conservation and carbon reduction formulated by the Executive Yuan. Its purpose is to integrate information services and uniformly dispatch information resources to satisfy the information operation needs of military units at all levels. However, it must be considered that resource centralization is a high risk. Therefore, how to explore the mainly indicators affecting the information security of the military cloud data center is an important issue through scientific methods. This study shows that the highest weight among three categories is “organizations and the professionals’ capabilities," in which the top three indicators with higher weights are "senior executives' awareness and support on information security," "personnel safety assessment," and "system operation and management capabilities." The findings of this study can be used as an important reference for the military cloud data center during designing information security specifications and implementing information security practices. As a whole, builds a dedicated cloud data center, the impact of "people" on information security is more important than "equipment" and "management"; therefore, improve the information security literacy of senior executives and implement assessment and evaluation of information Personnel competence and personnel training to make the developed system comply with the information security protection standards are top priority.

Keywords: Cloud Data Center, Information Security, Delphi Method, Analytic Hierarchy Process (AHP)

一、前言

隨著全球資訊科技的應用與發展日益普及化，資訊安全風險與網際網路日漸的提升，政府公家機構、民間企業及各項關鍵基礎設施，亦容易成為網路所攻擊目標。相對的我國對岸中國連年大幅度提高資電與網路作戰攻擊能量，威攝著我國各項軍、民網路體系。隨著我國國防預算相對有限、兵源縮小、難以獲取先進武器、並伴隨著網路資安威脅漸增、國家防衛意識趨漸變淡及全球複合型災害興起等課題，我國均亟待正視及慎重因應（國防部，2017）。

美國在 2015 年「國家安全戰略」內容中提到，國家安全、經濟安全和公共安全等 3 項網路空間安全威脅是亟需面對嚴峻的挑戰之一（國防部，2015）。

根據美國隱私權情報交換所數據顯示，資料外洩通報事件，由 2016 年 813 件減少至 2017 年 553 件，但遭到外洩的資料，由 2016 年 33 億筆攀升至 2017 年 49 億筆，增加近 16 億筆，2018-2019 年接連爆發數起超大型資料外洩事件，且部份案列為重覆發生，2017 至 2019 國內外重大資料外洩事件如表 1，其中包含知名入口網站雅虎在 2017 年 10 月，坦承曾經在 2013 年 8 月遭網路攻擊，約 30 億筆用戶個人資料外洩，造成社會大眾及用戶恐慌與不安，擔心個人資料遭有心人士不當使用。

表 1　2017-2020 年國內外重大資料外洩事件

年度	月份	案例	內容摘述
2017	1 月	臺北市政府	約 4 萬名員工個資外洩
	9 月	美國消費者信用評等機構 Equifax	外洩約 1.45 億美國民眾及 1,520 萬英國民眾的個人身分識別資料
	10 月	Yahoo	公告 2013 年外洩用戶資料約 30 億筆
	11 月	Uber	5,700 萬客戶及駕駛資料外洩
2018	1 月	挪威衛生局	300 萬筆病患資料外洩
	3 月	Facebook	5,000 萬個資遭外洩濫用
	4 月	杜拜叫車服務公司 Careem	1,400 萬名客戶個人資料外洩
	6 月	中國視頻共享網站 AcFun	近千萬用戶資料外洩
	7 月	新加坡保健服務集團	150 萬病患的個資外洩
	8 月	美國電信業者 T-Mobile	200 萬客戶資料外洩
	9 月	臺北市政府衛生局	公共衛生資訊管理系統上百萬筆民眾個資外洩
	10 月	香港國泰航空	940 萬客戶資料外洩
	11 月	貝殼放大股份有限公司	6 萬筆個資外洩
2019	1 月	新加坡網路服務商 Secur Solutions Group（SSG）	80 萬 8,201 名個資外洩

年度	月份	案例	內容摘述
	5 月	1111 人力銀行	20 萬筆個資外洩
	7 月	銓敘部	59 萬筆公務員個資遭外洩
	9 月	厄瓜多市場分析公司	2,000 萬筆個資外洩
	12 月	Facebook	2.67 億名用戶資料外洩
2020	4 月	Zoom 雲端視頻	53 萬筆 Zoom 用戶帳密外洩
	6 月	任天堂	16 萬用戶個資外洩
	10 月	104 人力銀行	592 萬筆個資外洩

資料來源：本表資料整理自 iThome

近年各國致力於國家資訊基礎建設規劃與構建，資訊網路安全已成為全球性的議題，隨著網際網路迅速發展與普及，網路攻擊事件頻傳，網路攻擊已逐漸成為軍事所看不見的攻擊方式，敵人可藉由網際網路攻擊，遲滯或癱瘓國家重要基礎建設，進而影響國軍戰力。

國防部為遵循行政院節能減碳與資訊機房共構政策，因應雲端運算科技快速發展，同時，提升國軍各單位資訊服務可用性、便利性，自民國 99 年起規劃適用國軍特性之資訊服務雲端運算架構，以因應各級人員資訊作業需求。並於 105 年以支援作戰區獨立作戰及提高服務存活度為前提，於軍網上規劃高靈活度、自動化、高安全及高可用性之國軍雲端資料中心，收容作戰區內資訊服務，統一調度運算、儲存及網路資源，提升運作效率及管理效能，重塑更靈活、即時、穩健、彈性之國軍資訊基礎建設(國防部，2015)。

國軍雲端資料中心現屬計畫與建置階段，架構及資訊安全防護作為仍在持續研議中，國防部規劃整併現有機房及興建資料中心，於我國本島劃分四區設立主要雲端資料中心乙座，南北地區另各設立次要雲端資料中心乙座，以「作戰區獨立作戰」指導及支援規模，建構符合國軍特性之雲端服務架構，提供效率高及存活性強之資訊服務。緣此，如何評估並確保雲端資料中心之資訊安全，為現階段重要的課題。經查閱相關文獻，僅吳世璋於 2016 年以「網路資料中心資訊安全防護能力評估指標之研究」為題，以「某國軍網路資料中心」為對象，探討網路資料中心資訊安全防護能力評估指標，惟未發現有針對國軍雲端資料中心資訊安全進行探討及評估之相關論文。

國軍相關單位刻正依國防部指導實施規劃及建置國軍雲端資料中心，故如何評估及落實資訊安全防護作為，在有限資源下，適時調整優先順序，提高服務及資料安全性與穩定度，防止國防資訊外洩或遭竊取、基礎建設遭破壞等攻擊，已成為國家與軍事安全重要之議題。在良好的資訊安全架構中為維護資料的機敏性、正確性、可用性以及完整性，電腦防護範圍應包含：有形設備如資訊主機房、主機、防火牆、網路線及無形的不可抗拒因素、電力、防火、軟(韌)體、資料及數據等事務，(劉國昌與劉國興，1995)。資訊安全為了確保資料或數據在傳遞或儲存過程中，遭有心人士新增、讀取、刪除或竄改，應將安全防護技術及管理工作程序運用在電腦的韌體、軟體、硬體、及資料（或數據）(黃亮宇，1992)。為瞭解國軍雲端資料中心資訊安全防護未來重點發展方向，朝重點建軍備戰，持續籌建可恃之國防資訊安全防護能力，期望藉由本研究可獲得國軍雲端資料中心資訊安全可供依循之評估指標。

二、背景知識與文獻探討

本研究的目的為探討國軍雲端資料中心資訊安全各構面項目，並運用層級分析發展資訊安全的評估衡量指標，以奠定國軍資通電整體環境基礎，創造資訊作業環境之效率及安全。因此，本次背景知識與文獻探討分為四大部分進行說明，首先第一部份為國軍雲端資料中心服務及架構說明；第二部份為資訊安全定義說明；第三部份為資訊安全管理制度及其作業規範說明；第四部份為資訊安全相關指標建構文獻的介紹。以下部份內容說明如下，藉以做為研究之基礎。

2.1 國軍雲端資料中心

在數位時代，企業進行電子化（e 化）的過程中，電子資料安全儲存一直是重要的課題；隨著各類資訊系統發展，以及近年大數據相關應用不斷增加，除了提高競爭力，企業也思考如何能以創新的方式，在兼顧降低成本與提升效率的前提下，妥善管理營運資料，以支持企業永續經營。

為妥善保存企業營運資料，完善的網路設備與資訊安全相關設施是必須的，然而，若要自行建置與維護各項資通訊設備，對各個企業而言卻是一項龐大沈重的負擔成本；所以，網路資料中心（Internet Data Center, IDC）就因應潮流而應運而生。所謂網路資料中心，可提供企業 e 化時存取及管理資訊，如同資料的銀行，亦稱一個大型數據及資訊儲存中心。網路資料中心所提供的服務可分類為二種模式，第一種將監控服務、網路管理、防火牆、伺服器加速快取服務、網路流量分析、設施管理、網路健診、網管委外基本服務及防毒、防駭等安全管理服務，做為網路加值服務；第二種提供企業用戶主機代管（Co-Location）、虛擬主機（Virtual Hosting）、機房共構及企業專線等服務，做為網路基本服務。

建置網路資料中心的成本，對民間企業是一大負擔，對國軍而言亦是如此。國軍資訊人力與資源，在過去數年間歷經多階段的精簡，以往由各軍種分散建置資訊機房的模式，現階段已面臨管理人力不足以及運作效率欠佳等諸多課題，實有必要以集中建置方式，將人力與資源向上收攏，並將資訊資源置於關鍵節點，使資訊服務能有效支援各單位任務遂行。

這樣的概念在雲端運算出現後，有了解決方案。國防部自民國 100 年起，逐步推動雲端服務的建構，期整併國軍現有資訊機房為國軍雲端資料中心及軍種資料中心，國軍資訊作業規劃由單點提供服務調整為作戰區導向之多點服務架構，資訊服務型態從過去各單位自行籌建、管理，調整為整體規劃發展，資訊服務由資料中心統籌提供，另規劃為 5 大類型，其類型可分為基礎建設、功能性服務、通用性服務、雲端資安及虛擬化（國防部，2011）。

2.1.1 雲端資料中心架構

在機房的可靠性、可用性的架構設計方面，國際機房標準機構(Uptime Institute)所制定的機房建置參考指南以及 TIA-942 所訂下的基礎設施標準，是常見被引用的設計依據。Uptime Institute 成立於 1993 年，將機房設計架構劃分為 4 個不同層級，主要是針對

電力、冷卻空調、維護以及故障承受力進行區分，Tier 1 採單迴路設計，僅需提供空間與電力，確保在正常的辦公時間內不會關閉；Tier 2 則要求電源開關及冷卻空調都要有冗餘的容量設計，以提供維護的餘裕，不會因為單一設備故障，而導致資訊流程中斷；而 Tier 3 則必須做到不需要關閉設備即可維護，在面臨停電或水路管線停止供水的情況下，仍可進行維護作業，而不會影響資訊服務運行；Tier 4 則建立在 Tier 3 的基礎之上，加入容錯（Fault Tolerance）設計，以 N+N 的架構，確保不中斷運行。

而 ANSI/TIA-942 則是以全方位的角度來思考資料中心電信基礎設施應該如何設計的標準規範。這項規範定義了空調、電力、消防、網路以及實體環境等各個層面，並且將標準要求設為 4 個 Rated 等級。Rated 1 僅提供基本的基礎設施，對設備的保護有限，Rated 2 應具有備援機制，例如 UPS 須採用並聯式，萬一其中一組 UPS 故障，將由另一組接替。Rated 3 要求可靠度更高，在這個等級中須具備二個饋電線路。Rated 4 等級設計更加完善，採用 2N 或 2N+1 機制，即使一半設備故障，至少還有一半可以運作。

這兩種設計架構驗證在國內都有典型的案例，例如中華電信在 105 年啟用的雲端資料中心，就引入了 ANSI/TIA-942-A Rated 4 & Rated 3 認證，而台灣大哥大的雲端資料中心則獲得了 Uptime Institute 的 Tier III 設計、建置與維運三階段認證。

行政院於 2017 年 1 月 9 日訂定「行政院及所屬各機關資料中心設置作業要點」(行政院，2017)，其目的為提升行政院所屬各機關（構）資料中心運作效率及管理效能，打造穩健、彈性及綠能之資訊基礎建設，該要點針對「資料中心」、「雲端資料中心」與「通訊機房」之定義，說明如下：

一、資料中心：指各機關為供資通訊系統正常運行所設置之基礎及備援設施，其主要設施包含運算伺服主機、儲存設備、網通設備、資安設備、環境控制設施及存放前述設施之實體空間。

二、雲端資料中心：指提供使用者 5 項服務特性，隨需自助服務（On-demand Self-service）、多元網路存取（Broad Network Access）、多人共享資源池（Resource Pooling）、快速且彈性部署（Rapid Elasticity）及服務可量測（Measured Service）之資料中心。

三、通訊機房：指各機關為提供員工連結網際網路、內部使用之資訊服務及維持與資料中心網路通訊，所設置之小型資料中心，其設施僅限必要之網通設備、資安設備及提供機關在地專用資通訊服務運行所需之運算伺服主機。

就前述「資料中心」與「雲端資料中心」的定義而言，前者著重於資訊機房的基礎設施與備援管理，而後者則是著重於為了提供存取服務而進行的設備建置與資源部署，因此，兩者在資訊安全管理上注重的面向應有所不同。在 2009 年以前，大部分的雲端運算基礎架構是由通過資料中心傳送的可信賴服務和建立在伺服器不同層次的虛擬化技術所組成。人們可以在任何有提供網路基礎設施的地方使用這些服務，而「雲端」通常表現為對所有用戶運算需求的單一存取點。人們通常希望商業化的產品能夠滿足服務品質（Quality of Service, QoS）的要求，並且一般情況下要提供服務水準協定（Service Level Agreement, SLA）。

2.2 資訊安全

隨著網路技術快速發展，且配合政府持續推動資訊化，國軍對於網路及資料科技依賴逐漸增加，因應資安事件頻傳及多樣化，強化資訊與網路安全及管理，為國軍持續努力精進之目標，本章節將針對資訊安全定義與國軍內部資訊安全政策等面向實施探討。

2.2.1 資訊安全定義

資訊安全的定義，最早由 IBM (1984) 公布之 IBM Data Security Support Programs 提出，對於資訊資產有意或無意的情形下，未經授權公開、修改、破壞或使之失效等行為的防護。資訊安全的定義，學者多有不同的見解，國內外學者研究定義如表 2，而資訊安全的目標，就是保護儲存資料或資訊之機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）。

一、機密性（Confidentiality）：保護資訊免向未經授權人士披露。

二、完整性（Integrity）：保護資訊免受未經授權人士更改。

三、可用性（Availability）：讓資訊可供已獲授權人士在需要時取用。

表 2　資訊安全定義整理表

來源	年份	定義
IBM	1984	對資訊資產有意或意外的情況下，未經授權的公開、修改、破壞或使之失效等行為的防護。
黃亮宇	1992	就是把管理程序和安全防護技術應用於電腦的硬體、軟體和數據（或資料）上，以確保儲存或傳遞中的數據（或資料）免除他人有意或無意的讀取、增刪或修改。
Russell & Gangemi	1992	保護任何與電腦有關的事務之安全，將管理程序與安全防護技術運用在硬體、軟體與資料中。
劉國昌	1995	電腦安全的保護範圍包括：機房、電腦主機、終端機、電腦網路線、軟體與資訊等有形或無形的電腦相關事務，良好的安全措施維護了這些資料的機密性、正確性、可用性及完整性。
國家標準 CNS27002	2007	使資訊不受廣泛的威脅之保護，以確保營運持續性、降低營運風險至最低、得到最豐厚的投資報酬率及最大商機。
周宣光	2007	資訊安全是指用來防止非法存取、竄改、偷竊和對資訊系統造成傷害的一些政策、程序和方法，藉由一些技術和工具來保護硬體、軟體、通訊網路和資料以提升資料的安全性。
ISO 27001	2013	資訊安全包括三個主要方面：機密性、可用性和完整性，其包含適當考慮廣泛威脅的安全措施之應用和管理，以確保業務成功和持續的目標，並最大限度地減少資訊安全事件的影響。

資料來源：本研究整理

資訊安全分為三種：「硬體安全」，包含電腦硬體環境控制、機房管理、硬體設備使用安全；「軟體安全」，包含系統安全、應用程式安全及個人資料安全；「個人安全」，包含人身安全、個人隱私安全及網路通訊安全（張博竣，2004）。

一般而言，資訊安全的定義就是將任何與電腦相關之事物保護並維護運作，資訊是指將眾多資訊藉由整理或分析的過程，使其成為有意義之內容，具有價值及重要性之資訊也將成為決策制訂之參考依據（葉乃菁與李順仁，2004）。

吳世璋於 2016 年進行網路資料中心資訊安全防護能力評估指標之研究，以國軍某

網路資料中心為例，運用專家問卷歸納出適合國軍在執行網路資料中心資訊安全防護時所需的構面項目，透過 AHP 建立網路資料中心資訊安全防護能力標準的評估標準權重，並建立評估表，透過專業人員評分，再依評分結果做為網路資料中心後續資訊安全發展方向參考，發現主要構面以設備建置最高，針對整體指標權重排序又以備份備援系統、傳輸保密裝及門禁安全設施最為重要（吳世璋，2016）。

三、研究方法

3.1 研究步驟

本研究的步驟首先確定研究問題及目的，並透過文獻分析針對資訊安全指標進行整理及歸納，初擬國軍雲端資料中心資訊安全構面及指標，再運用德爾菲法實施專家意見調查，加以分析及篩選指標，最後以 AHP 建立權重體系問卷實施調查，獲得各構面及指標的相對重要性及權重。資訊安全評估指標為多個評估準則之決策問題，為使複雜且非結構化的問題逐漸系統化，了解因素之間的相對重要性關係，求得各個方案的權重值，提供決策者選擇適當方案的參考，本研究採用層級分析法(AHP)來建立權重體系設計問卷並調查，依據回收問卷實施統計分析與 Expert Choice 11 AHP 專家決策分析軟體執行權重計算，並整理歸納出研究成果，最後提出研究步驟如圖 1 所示。

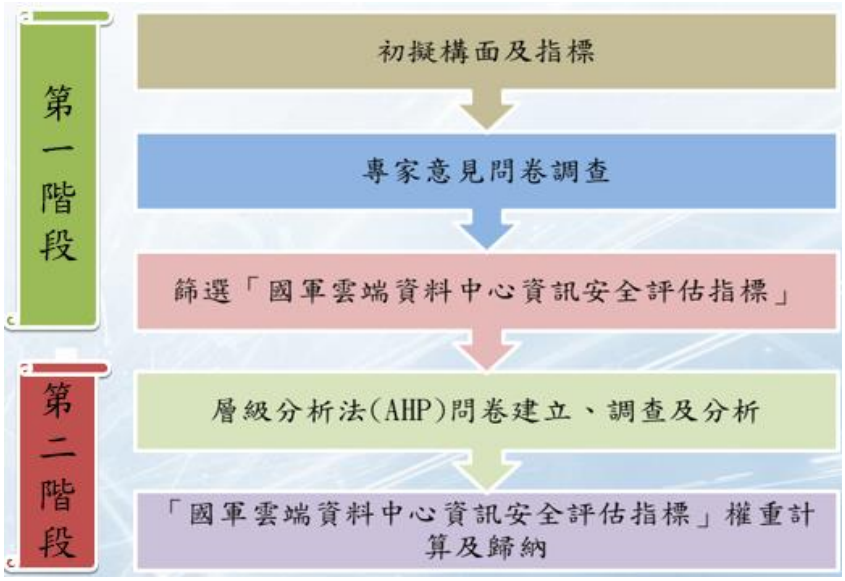

圖 1　研究步驟

資料來源：本研究整理

3.2 研究設計

本研究運用層級分析法建立「國軍雲端資料中心資訊安全評估指標」，流程區分三個部分，(一)建立層級架構。(二)問卷設計與量表選定。(三)實施方式，分述如後：

3.2.1 建立層級架構

本研究先期從二個方向進行文獻蒐集、分析與歸納：

- 網路資料中心構建之相關文獻：

透過文獻資料庫搜尋相關文獻，包括全國博碩士論文摘要索引系統、中華民國期刊論文索引影像系統等資料庫，以「網路資料中心」(IDC)、「資訊安全管理」(Information

security Management)、「標準」(Standard)、「資訊素養」(Information Literacy)、「資訊安全」(Information Security)、資訊安全素養(Information Security Literacy) 、「資訊安全」（Information Security）等關鍵字搭配查詢。進行文獻蒐集、分析與歸納。

- 指標體系建構方法之相關文獻：

搜尋與資訊安全指標體系建構有關之博碩士論文、期刊、學術雜誌，並加以歸納、分析，進而決定本研究之研究設計。參考林志章(2015)「國軍網路作戰部隊作戰能力評估指標」、吳世璋(2016)「網路資料中心資訊安全防護能力評估指標之研究-以國軍某網路資料中心為例」及行政院雲端資料中心提供之資訊安全機制，綜整出「國軍雲端資料中心資訊安全評估指標」構面，再透過資訊安全防護相關文獻探討，產生第三層評估準則，參考文獻彙整如表 3。

表 3　國軍雲端資料中心資訊安全評估指標構面及準則參考文獻彙整表

年份	研究者或出處	題目及內容概要
2011	林麗娟	建構企業導入雲端運算資訊架構評估指標 1.系統安全。 2.資訊安全檢驗。 3.認證與授權。 4.訊息保護。 5.資料備份回存。 6.災害回復計畫。 7.偵測與監控。
2011	張至伶	企業導入雲端運算環境的資訊安全因素之研究 1.資訊安全的組織。 2.通訊與作業管理。 3.存取控制。 4.資訊系統獲取、開發及維護。 5.營運持續管理。 6.遵循性。
2014	葉謦瑞	企業導入虛擬化之資訊安全風險項目研究 1.設備維護標準作業。 2.進出存取權限管理。 3.實體資產保護與管理。 4.威脅弱點分析。 5.定期風險評鑑作業。 6.事件記錄後之追蹤改善。 7.資安管控流程計畫。 8.建立緊急聯繫機制。 9.資安人員的專業性。

		10.資安系統穩定程度。 11.網路傳輸管理。 12.備援機制。 13.通訊安全作業。 14.CA認證與憑證管理。 15.資訊備份作業。
2015	林志章	國軍網路作戰部隊作戰能力評估指標 1.網路封包分析。 2.電腦鑑識操作。 3.資訊安全設備。 4.誘捕系統操作。 5.網路安全設備。
2016	行政院	雲端資料中心提供之資訊安全機制 1.入侵偵測防禦系統。 2.惡意黑名單阻擋。 3.惡意活動偵測。 4.防毒控管及主機防毒。 5.主機及網站弱點掃瞄。 6.作業系統安全修正檔更新通知。 7.服務監控及告警。 8.不同用戶虛擬主機安全隔離。
2016	吳世璋	網路資料中心資訊安全防護能力評估指標之研究－以國軍某網路資料中心為例 1.備份備援系統。 2.傳輸保密裝備。 3.門禁安全設施。 4.資安系統。 5.網路基礎設施。 6.網路安全管理能量。 7.系統操作能力。 8.內部訓練制度。
2016	陳志誠 、 劉用貴	建構雲端環境資料安全存取模型暨績效評估 1.使用者身分認證。 2.資料儲存與安全隔離。 3.雲端優先權多級安全排程。 4.資料安全存取與隱私保護。 5.資料安全傳輸。

資料來源：本研究整理

綜合歸納初步評估指標要項，找出所有可能影響國軍 IDC 資訊安全防護能力評估之因素，將影響因素區分為三個層級。本研究將影響國軍雲端資料中心資訊安全評估之因素，區分為三個層級，第一層為本研究之目標，資訊安全評估指標之建立，第二層為主要構面，第三層為評估準則，如圖 2 所示。

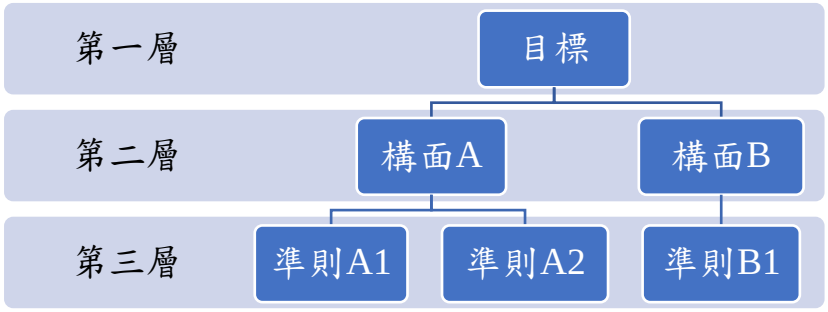

圖 2　層級架構示意圖

資料來源：本研究整理

經過文獻探討整理出第二層主要構面要素為「資訊安全設備」、「資訊安全管理」及「組織與人員專業能力」等 3 大構面， 第三層則是國軍雲端資料中心參酌文獻所整理的資訊安全防護能力評估所必須考量的 25 個細部指標，如圖 3 所示。

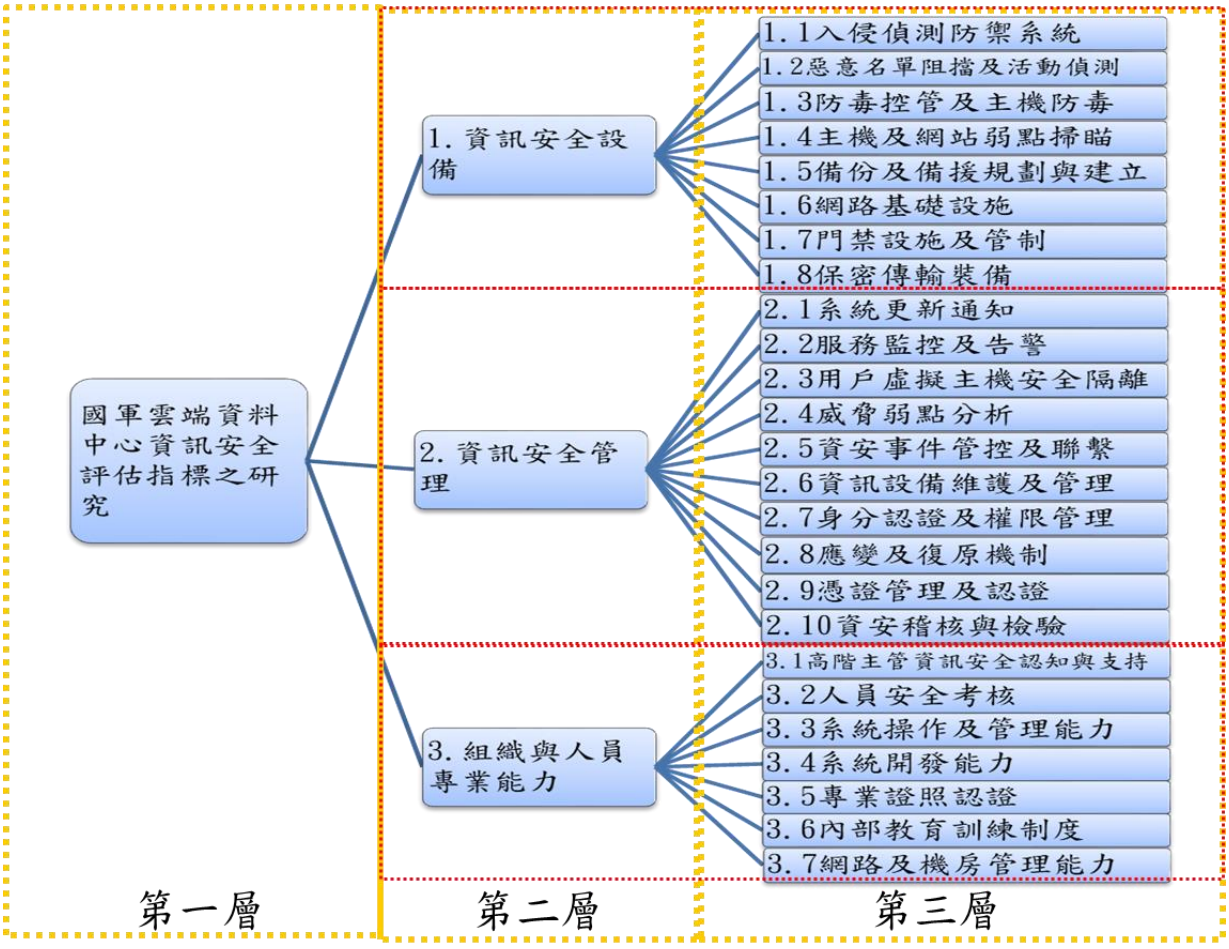

圖 3　因素層級指標項目

3.2.2 問卷設計與調查

本研究所探討對象為國軍雲端資料中心，現屬計畫階段，相關服務、架構及資訊安全防護作為仍在發展與建置中，國防部規劃整併現有機房及興建資料中心，於本島劃分四區設立主要雲端資料中心乙座，南北地區另各設立次要雲端資料中心乙座，以「作戰區獨立作戰」指導及支援規模，建構符合國軍特性之雲端服務架構，提供效率高及存活性強之資訊服務。

本研究區分二階段實施問卷設計與調查，指標擬訂發展流程如下：

一、第一階段德菲爾專家問卷：

(一)問卷調查

依文獻探討綜整產生初擬構面與準則，擬訂第一階段評估指標問卷，為使研究結果符合實務需求，本階段問卷由「國防部及軍種司令部高司單位資訊部門」及「實際從事資訊機房資訊安全防護作業」等專業人員實施抽樣問卷調查，評估各指標之重要性，並區分「決策」、「督導」及「執行」等類別，對象以具資訊專業證照 2 張以為優先，證照不足者，需具備碩士或指參班以上學歷，且實際從事資訊相關職務年資達 10 年以上人員，共計抽取 30 位專業人員實施問卷調查，統計回收問卷 29 份，回收率 96.67%，調查對象階級計有將官 1 員、校官 23 員、尉官 4 員、士官長 1 員；服務全年資達 21 年以上 5 員、16-20 年 15 員、10-15 年 4 員、10 年以內 5 員，問卷回收統計表如表 4。

表 4　第一階段問卷回收統計表

類別	職務	階級	年資	人數	發送份數	回收份數	回收率
決策	高司幕僚政策主管	將官	21 年以上	1	1	1	100%
督導	高司幕僚政策主管	校官	21 年以上	2	2	2	100%
決策	高司幕僚政策主管	校官	21 年以上	2	2	2	100%
決策	高司幕僚政策主管	校官	16-20 年	2	2	1	50%
督導	資訊機房資訊主管	校官	16-20 年	2	2	2	100%
執行	高司幕僚政策參謀	校官	16-20 年	11	11	11	100%
執行	高司幕僚政策參謀	校官	10-15 年	2	2	2	100%
執行	高司幕僚政策參謀	校官	10 年以內	1	1	1	100%
執行	資訊機房資訊參謀	校官	16-20 年	1	1	1	100%
執行	資訊機房資訊參謀	校官	10-15 年	1	1	1	100%
執行	高司幕僚政策參謀	尉官	10 年以內	4	4	4	100%
執行	高司幕僚政策參謀	士官長	10-15 年	1	1	1	100%
	回收 29 份，回收率 96.67%						

資料來源：本研究整理

(二)問卷分析

本階段依業務單位特性區分「決策」、「督導」、「執行」等不同階層及職務調查，以結合實務經驗及需要，首先第一階段採用德爾菲法專家問卷，除高司幕僚政策參謀 1 員，建議構面修正為「政策」、「管理」、「技術」外，餘均對第二層構面無修訂意見，考量問卷係由文獻蒐集彙整而來，且大部分專家均表示同意，故不予修正，將納入未來研究方向參考。

二、第二階段 AHP 問卷

依第一階段德菲爾專家問卷，統計分析獲得指標，發展第二階段 AHP 問卷，以瞭解資訊安全關鍵指標，本研究評量方式使用李克特量表(Likert Scale)做為量化指標的測量工具。李克特量尺可以當它是一把尺，常用的刻度有 3 至 11 點量尺，本研究採用李克特七點尺度量表衡量，每個選項對應一個數值，這些數值具有方向性，可將數值設定愈高表示愈滿意或愈低則愈不滿意，且應符合「點到點之間等距」特質，數值之間除應有次序關係外，亦應具有等距的特質，其格式及給分方式如表 5。

表 5　量尺對照格式及給分方式

問題面向	非常同意	同意	有點同意	普通	有點不同意	不同意	非常不同意
正向問題	7	6	5	4	3	2	1
反向問題	1	2	3	4	5	6	7

資料來源：本研究整理

3.3 評估比較

依據問卷調查產生統計之結果，執行各層級準則間權重計算，此階段分為三個方式。

3.3.1 建立成對比較矩陣

因素的成對比較，係指對其上一層級某一要素做為評估準則時，進行要素間的成對比較，比較兩個要素間的相對重要程度，假設有 n 個因素時，則需進行 n(n-1)/2 個成對比較，成對比較矩陣如下所示：

$$[A] = [a_{ij}]_{n*n} = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{12} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \cdots & 1 \end{bmatrix} \quad (1)$$

a_{ij}=相對權重

3.3.2 計算特徵向量及特徵值

將建立完成之成對比較矩陣，透過數值分析中常用之特徵向量理論基礎，計算出特徵向量值及特徵值，並求得各層級準則間之相關權重，Saaty 提出四種近似法求取向量值，其中列向量平均值的標準化，可求得較高精確的數值，計算公式如下：

$$W_i = \frac{\left(\prod_{j=1}^{n} a_{ij}\right)^{\frac{1}{n}}}{\sum_{i=1}^{n}\left(\prod_{j=1}^{n} a_{ij}\right)^{\frac{1}{n}}} \qquad i,j = 1,2,\ldots,n \quad (2) \qquad (2)$$

3.3.3 一致性檢定

問題決策時，判斷的一致性是非常重要的。如果 A 比 B 重要，B 又比 C 重要，理論上來說 A 應該比 C 重要，但在實際狀況中，進行成對比較時，評估者要達到前後一

致是不容易的，一致性檢定目的在檢驗評估者整體比較過程中，所做判斷的合理程度，對於各要素間權重判斷是否一致，結果是否可信，誤差值是否在可接受的範圍中。

一個好的衡量工具，應具有足夠的信度，AHP 在信度檢定，是採用一致性指標

$$\text{C. I.} = \frac{\lambda_{max} - n}{n - 1} \tag{3}$$

$$\lambda_{max} = \frac{1}{n}\left[\frac{Z_1'}{Z_1} + \frac{Z_2'}{Z_2} + \cdots + \frac{Z_n'}{Z_n}\right] \tag{4}$$

λ_{max}=最大特徵值

(Consistence Index, C.I.)及一致性比率(Consistency Ratio, C.R.)來檢定，若 C.I.=0 表示評估者前後判斷完全一致，C.I.值越小表示一致性愈高，C.I.值越大時表示前後判斷不一致性越高。本研究以 Expert Choice 11 分析軟體進行計算，在一致性檢定時，Saaty 建議 C.I.≦0.1 時，為可接受的誤差範圍內，檢定公式如下：

$$\text{C. R.} = \frac{C.I.}{R.I.} \tag{5}$$

當層級中因素數量增加時，判斷相對將增加，成對的矩陣階數也多，將使判斷不容易維持一致性。根據 Dak Ridge National laboratory 與 Wharton School 的研究，從評估尺度 1-9 所產生的正倒矩陣，在不同的階層數下，產生不同的 C.I.值，稱為隨機指標(Random Index, R.I.)，其值隨矩陣階數之增加而增加（鄧振源、曾國雄，1989）。而 C.I.值與 R.I.值的比率，稱為一致性比率(Consistency Ratio, C.R.)，公式如下：

因此在 C.R.值在≦0.1 時，表示矩陣一致性程度是很高的。其隨機指標數值如表 6：

表 6　隨機指標數值表

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

資料來源：Saaty, 1980

3.4 小結

本研究透過文獻蒐整及分析，擬訂國軍雲端資料中心資訊安全構面及指標，經由專

家意見修訂及篩選指標，並使用 AHP 建立權重體系問卷實施問卷調查，再經由建立成對比較矩陣、計算特徵值與特徵向量及一致性檢定等 3 個步驟，完成各層級要素間權重計算，以利整體層級權重計算及分析。

四、研究結果與討論

4.1 AHP 問卷資料統計及分析

在第一階段所使用德菲爾法專家問卷所獲得數據結果，透過 AHP 建立為第二階段權重問卷，第二階段針對國防部、各軍種司令部、指揮部及資訊機房管理資訊人員實施調查，問卷調查對象維持第一階段發放對象區分為決策、督導及執行階層，階級以軍官及上士以上士官為主，問卷計發出 181 份，回收 181 份，扣除一致性檢定未達可接受誤差值(C.I.≦0.1)，無效問卷 32 份，有效問卷 149 份，有效問卷人員基本資料統計分析如表 7。

表 7　問卷調查對象統計表

類別	階級	發放 問卷數	回收 問卷數	有效 問卷數	無效 問卷數
決策階層	上校	4	4	4	
	中校	7	7	7	
	少校	15	15	14	1
管理階層	中校	10	10	9	1
	少校	21	21	18	3
	尉官	4	4	4	
	士官長	11	11	8	3
執行階層	少校	11	11	7	4
	尉官	38	38	34	4
	士官長	28	28	19	9
	上士	32	32	25	7
合計		181	181	149	32
問卷回收率 100%、有效率 82.32%					

資料來源：本研究整理

第二階段問卷使用 Expert Choice 11 為主要統計及分析工具，以產生各階層一致性指標(Consistency Index, C.I.)及一致性比率(Consistency Ratio, C.R.)，以利判斷矩陣一致性是否符合要求，如 C.R.≦0.1 代表數值為可接受之範圍，亦表示矩陣具有一致性比率。

4.1.1 主要構面分析

「主要構面」部分，經由問卷權重調查統計分析顯示「組織與人員專業能力」為最重要，其次為「資訊安全管理」,「資訊安全設備」再次之，一致性檢定 C.I.值為 0.01，C.I.值≦0.1，代表成對比較時矩陣的一致性為可接受的範圍，一致性比率 C.R.值為 0.017，C.R.值≦0.1。

透過 AHP 問卷調查得知，主要構面權重比率以「組織與人員專業能力」35%最高(圖

4)，代表雲端資料中心對於組織制度、人員考核及專業能力的要求較一般資料中心更高，因為雲端資料中心不僅只是存放資料，更支援 3 種服務模式及 4 種佈署方式，都將大幅度的提高組織及人員的能力需求。

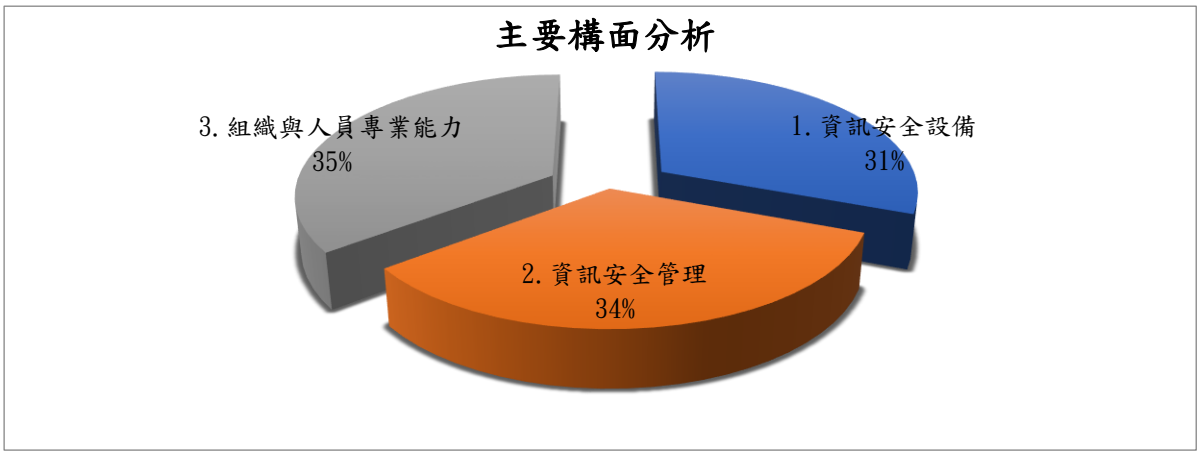

圖 4　主要構面分析圖
資料來源：本研究整理

4.1.2 資訊安全設備構面分析

「資訊安全設備」構面，經由問卷權重調查統計分析顯示「備份與備援規劃與建立」指標為最重要，接續依次序為「入侵偵測防禦系統」、「惡意名單阻擋及活動偵測」、「防毒控管及主機防毒」、「保密傳輸裝備」、「主機、網站及網段掃描」、「門禁設施及管制」及「設備產地與安全認證」，一致性檢定 C.I.值為 0.00099，C.I.值≦0.1，代表成對比較時矩陣的一致性為可接受的範圍，一致性比率 C.R.值為 0.00068，C.R.值≦0.1。

透過 AHP 問卷調查得知，資訊安全設備構面權重比率以「備份與備援規劃與建立」為 13%最高(圖 5)，顯示雲端資料中心備份及備援機制的重要性，服務不中斷及資料保存為單位重點工作，備份及備援如同單位的保險，能確保發生重大事故時，組織服務能持續不間斷，且保有原本的資料，使運作不受影響，降低潛在風險。

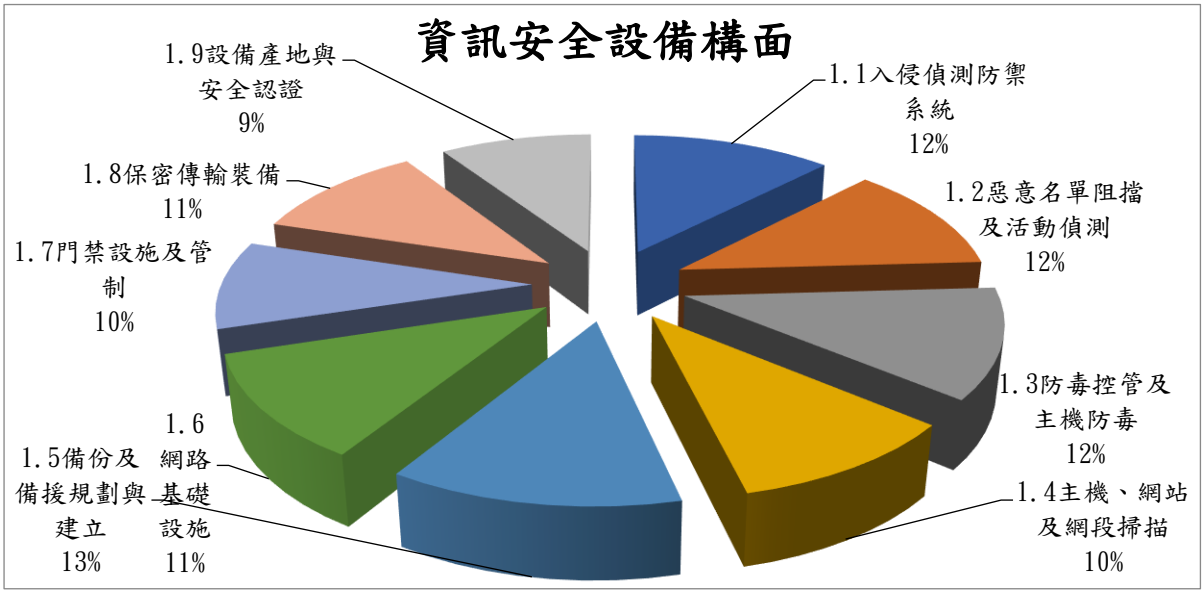

圖 5　資訊安全設備構面分析圖
資料來源：本研究整理

4.1.3 資訊安全管理構面分析

「資訊安全管理」構面，經由問卷統計分析顯示「身分認證及權限管理」指標最重要，接續依次序為「應變及復原機制」、「憑證管理及認證」、「威脅弱點分析」、「資安事件管控及聯繫」、「資安稽核與檢驗」、「系統更新通知及管理」、「服務監控及告警」、「用戶虛擬主機安全隔離」及「資訊設備維護及管理」，一致性檢定 C.I.值為 0.00063，C.I.值≦0.1，代表成對比較時矩陣的一致性為可接受的範圍，一致性比率 C.R.值為 0.00033，C.R.值≦0.1。

透過 AHP 問卷調查得知，資訊安全管理構面權重比率以「身分認證與權限管理」為 12%最高(圖 6)，顯示雲端資料中心身分認證及權限管理重要性，在雲端運用中，各項服務應用都依賴使用者帳號及身分，一旦使用者身分遭到冒用，將對單位運作及資訊安全造成重大衝擊。因此選擇高強度的身分認證方式，並事先了解可能面臨的安全風險，絕對是單位重要的課題，尤其權限管理為雲端服務之基礎，嚴密身份認證機制，避免產生以前所未發生的資安風險，這是所有採取雲端服務的單位，須有的認知及挑戰。

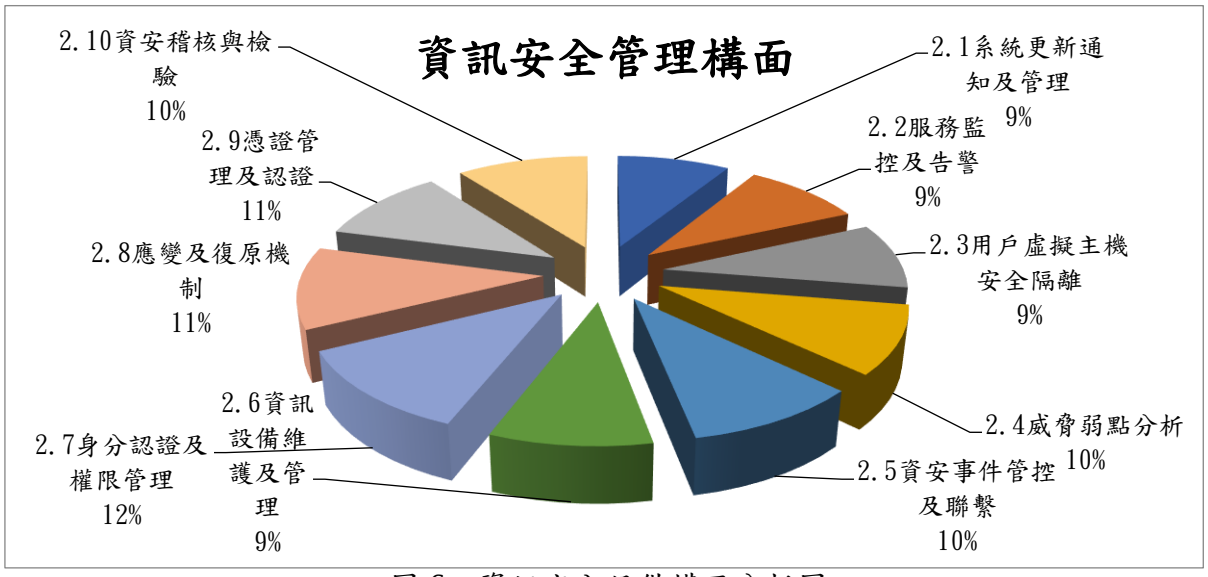

圖 6　資訊安全設備構面分析圖
資料來源：本研究整理

4.1.4 組織與人員專業能力構面分析

「組織與人員專業能力」構面，經由問卷權重調查統計分析顯示「高階主管資訊安全認知與支持」指標為最重要，接續依次序為「人員安全考核」、「系統操作及管理能力」、「系統開發能力」、「網路及機房管理能力」、「內部訓練及法規宣教」及「專業證照認證」，一致性檢定 C.I.值為 0.00153，C.I.值≦0.1，代表成對比較時矩陣的一致性為可接受的範圍，一致性比較 C.R.值為 0.00115，C.R.值≦0.1。

透過 AHP 問卷調查得知，組織與人員專業能力構面權重比率以「高階主管資訊安全認知與支持」為 18%最高(圖 7)，高階主管在單位中擔任資源分配調整及溝通協調角色，且對於新科技資訊技術的採用，具有相當程度之影響力，本研究與 Chatterjee et al.(2002)研究發現高階主管的倡導為影響企業採用新科技的關鍵要素相符，且 Choe(1996)及 Weill and Olson(1989)也曾指出在過去資訊科技採用經驗中，高階主管的支

持是企業衡量資訊技術是否投資的重要因素。

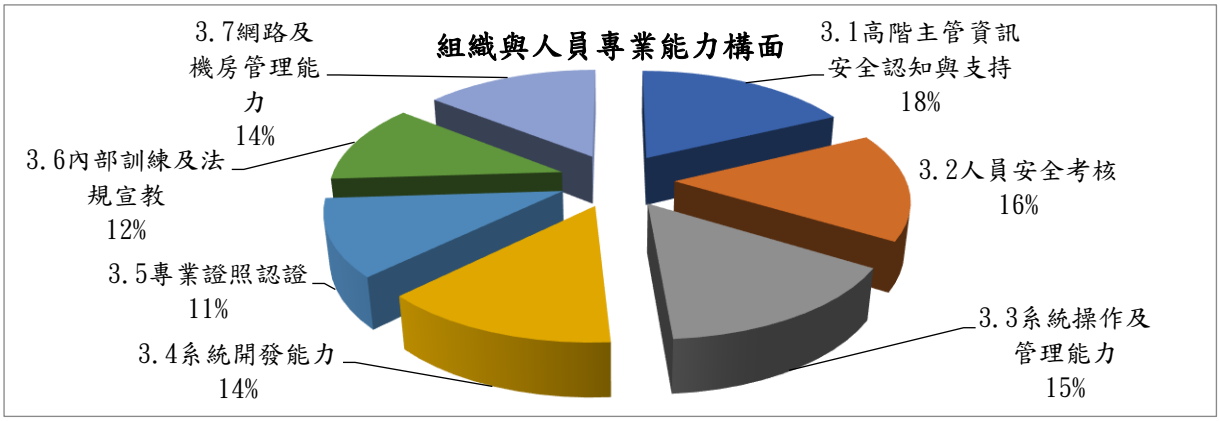

圖 7 組織與人員專業能力構面分析圖

資料來源：本研究整理

4.1.5 整體權重分析

本研究整體權重計算是依據 AHP 的列向量幾何平均值標準化實施彙整，將第三層準則所得權重數，與第二層構面權重比相乘，獲得整體權重，權重分析彙整表如表 8。整體權重調製為分析圖後，各準則之權重百分比如圖 8，由百分比圖發現，「高階主管資訊安全認知與支持」及「人員安全考核」為重要評估項目，所佔比率較高，其次為「系統操作及管理能力」、「系統開發能力」及「網路及機房管理能力」，也顯示人員的考核及專業能力之重要性。

表 8 國軍雲端資料中心資訊安全評估指標權重分析彙整表

層級	AHP 評估指標				
	評估指標		層級權重	整體權重	整體排序
1	國軍雲端資料中心資訊安全評估指標		1		
2	資訊安全設備		0.307	0.307	3
	資訊安全管理		0.339	0.339	2
	組織與人員專業能力		0.354	0.354	1
3	資訊安全設備	入侵偵測防禦系統	0.123	0.038	11
		惡意名單阻擋及活動偵測	0.118	0.036	13
		防毒控管及主機防毒	0.119	0.037	12
		主機、網站及網段掃描	0.103	0.032	21
		備份及備援規劃與建立	0.126	0.039	9
		網路基礎設施	0.113	0.035	16
		門禁設施及管制	0.096	0.029	25
		保密傳輸裝備	0.109	0.033	18
		設備產地與安全認證	0.093	0.029	26
	資訊安全管理	系統更新通知及管理	0.089	0.035	15
		服務監控及告警	0.094	0.030	24
		用戶虛擬主機安全隔離	0.092	0.032	20
		威脅弱點分析	0.095	0.031	22
		資安事件管控及聯繫	0.099	0.032	19
		資訊設備維護及管理	0.09	0.034	17

		身分認證及權限管理	0.117	0.031	23
		應變及復原機制	0.114	0.040	7
		憑證管理及認證	0.105	0.039	10
		資安稽核與檢驗	0.104	0.036	14
	組織與人員專業能力	高階主管資訊安全認知與支持	0.178	0.063	1
		人員安全考核	0.159	0.056	2
		系統操作及管理能力	0.152	0.054	3
		系統開發能力	0.138	0.049	5
		專業證照認證	0.113	0.040	8
		內部訓練及法規宣教	0.117	0.041	6
		網路及機房管理能力	0.143	0.051	4

資料來源：本研究整理

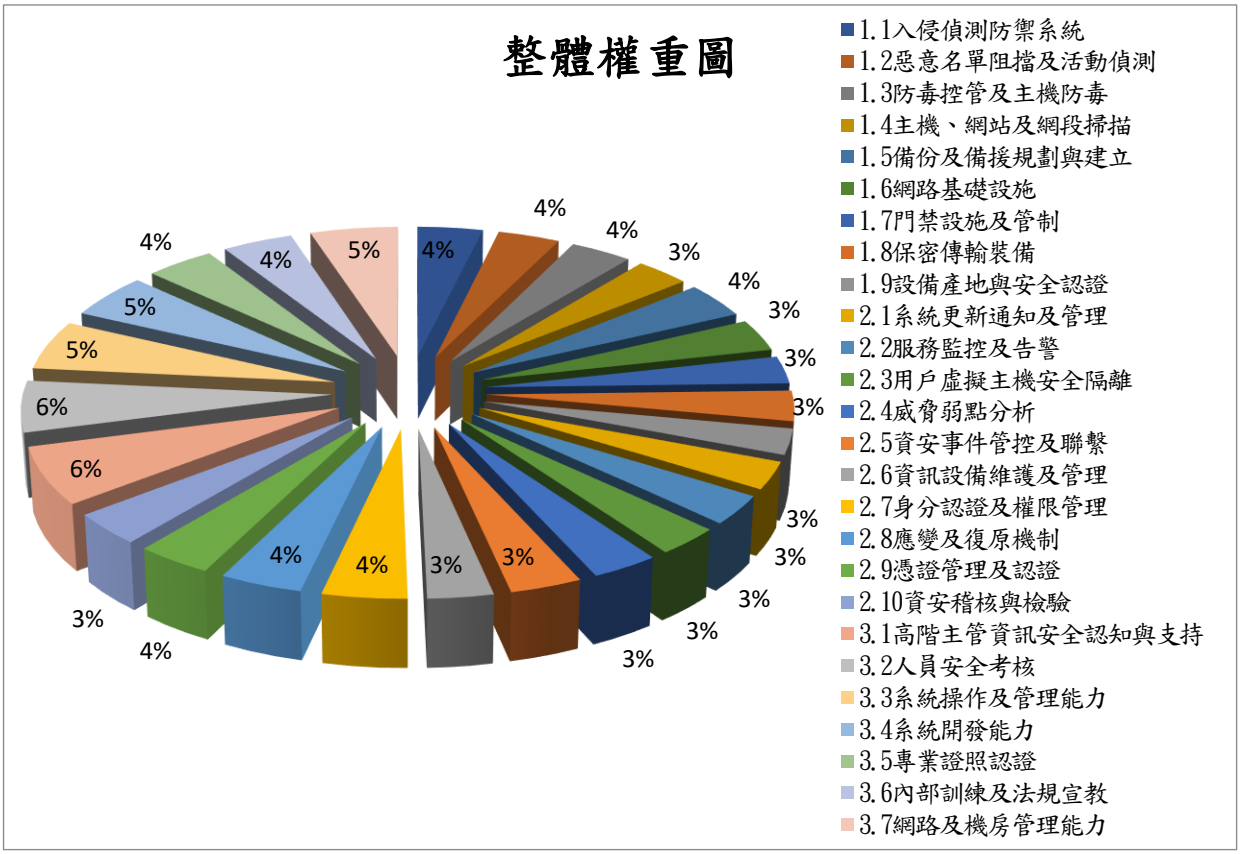

圖 8　整體權重分析圖

資料來源：本研究整理

依據 Expert Choice 11 軟體所產生之國軍雲端資料中心資訊安全評估指標整體權重圖如圖 9，整體權重以「高階主管資訊安全認知」最為重要，接續依次序為「人員安全考核」、「系統操作及管理能力」、「網路及機房管理能力」、「系統開發能力」、「內部訓練及法規宣教」、「應變及復原機制」、「專業證照認證」、「備份及備援規劃與建立」、「憑證管理及認證」、「入侵偵測防禦系統」、「防毒控管及主機防毒」、「惡意名單阻擋及活動偵

測」、「資安稽核與檢驗」、「系統更新通知及管理」、「網路基礎設施」、「資訊設備維護及管理」、「保密傳輸裝備」、「資安事件管控及聯繫」、「用戶虛擬主機安全隔離」、「主機、網站及網段掃描」、「威脅弱點分析」、「身分認證及權限管理」、「服務監控及告警」、「門禁設施及管制」、「設備產地與安全認證」，其中「組織與人員專業能力」構面項下 7 個指標，排序均為整體權重前 8 名，顯見國軍資訊人員認為該構面及指標為國軍雲端資料中心資訊安全應注意及強化面向。

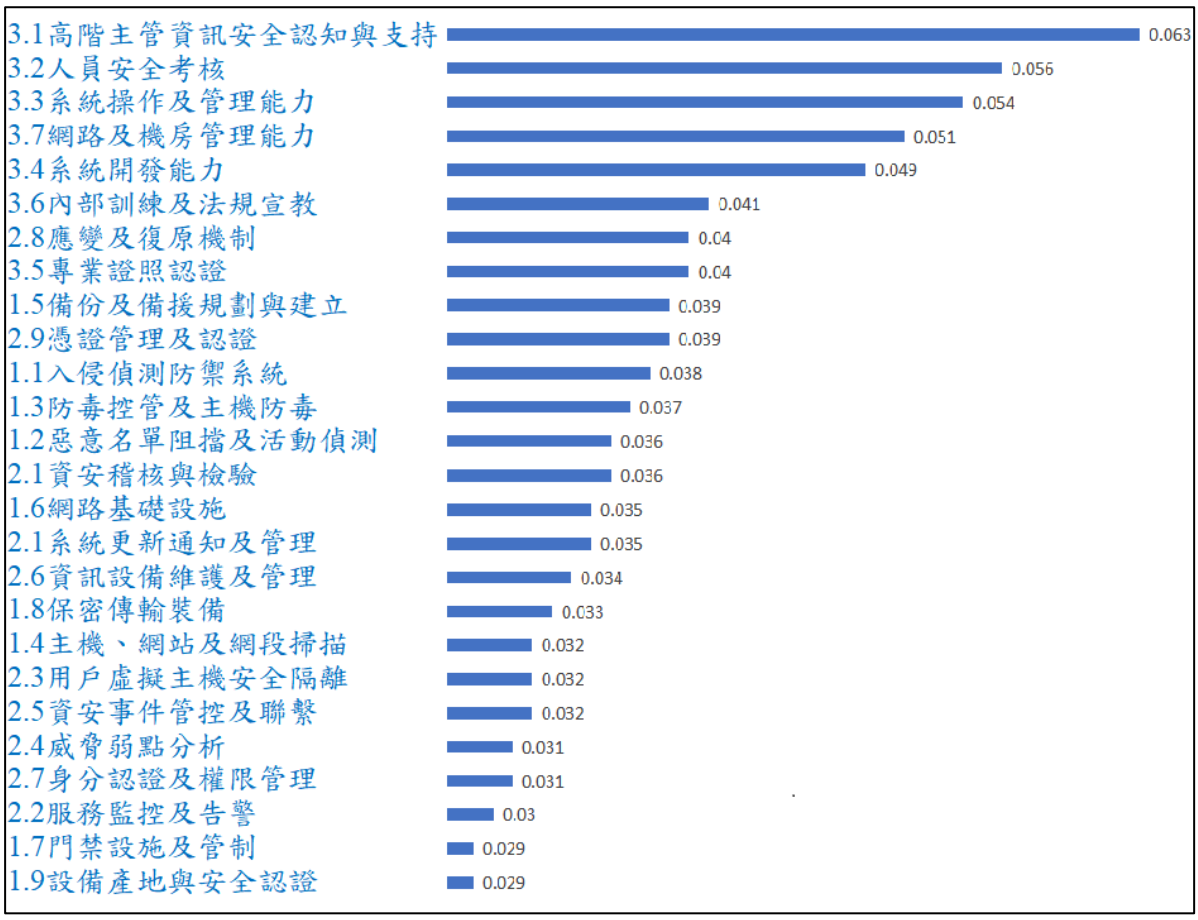

圖 9　整體權重排序圖

(資料來源：本研究整理)

4.2 比較分析

雲端資料中心所提供的服務，除網路資料中心基本服務及加值服務外，並包含雲端運算技術，依行政院及所屬各機關資料中心設置作業要點之定義，「資料中心」著重於資訊機房基礎設施與備援管理，「雲端資料中心」著重於提供存取服務而進行之設備建置與資源部署，本研究均與吳世璋(2016)「網路資料中心資訊安全防護能力評估指標之研究」實施對比，兩者除研究對象及層級、軟硬體規劃與設置不同外，且近年雲端運算技術逐漸成熟，行政院及國內雲端資料中心陸續啟用，促使國防部對於雲端資料中心建置要求及規劃越趨明確及周延，另雲端資料中心是由網路資料中心演進而來，期透過比較及分析瞭解「網路資料中心」及「雲端資料中心」在資訊安全管理應注意面向之差異。

經對照該論文經由文獻探討及德爾菲法專家問卷所得結果，研訂國軍網路資料中心

資訊安全防護各構面項目，其運用 AHP 發展資訊安全防護各構面能力評估之衡量標準，再透過評估指標的建構，進而獲得資訊安全防護能力的重要評估指標。

4.2.1 主要構面

吳世璋(2016)網路資料中心資訊安全防護能力評估指標主要構面權重以「設備建置」為最重要、「人員技術」次之、「管理程序」再次之，與本研究所得權重順序為「組織與人員專業能力」、「資訊安全管理」、「資訊安全設備」不同（主要構面權重分析比較表如表 9），吳世璋研究個案以國軍某軍種司令部網路資料中心為對象，與本研究以國軍整體雲端資料中心為主體不同，且國軍雲端資料中心係參考軍種司令部網路資料中心及國內雲端資料中心設備及架構，並委託專業廠商評估後規劃建置，且雲端運算的導入，將對組織運作帶來變革，增加人員專業能力需求，故兩者調查結果優先順序不同。

表 9　主要構面權重分析比較表

權重排序	研究者及題目	
	吳世璋 網路資料中心資訊安全防護能力評估指標之研究— 以國軍某網路資料中心為例	本研究 國軍雲端資料中心資訊安全評估指標之研究
1	設備建置	組織與 人員專業能力
2	人員技術	資訊安全管理
3	管理程序	資訊安全設備

資料來源：本研究整理

4.2.2 整體權重

整體指標權重分析，吳世璋(2016)調查結果以「備份備援系統」、「傳輸保密裝備」、「門禁設施」較為重要，本研究所得權重依排序為「高階主管資訊安全認知與支持」、「人員安全考核」、「系統操作與管理能力」，「備份及備援規劃與建立」排序第 9、「保密傳輸裝備」排序第 18、「門禁設施及管制」排序第 24（整體權重排序比較如表 10）。

表 10　整體權重排序比較表

權重排序	研究者及題目	
	吳世璋 網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例	本研究 國軍雲端資料中心資訊安全評估指標之研究
1	備份備援系統	高階主管資訊安全認知與支持
2	傳輸保密裝備	人員安全考核
3	門禁安全設施	系統操作及管理能力
4	資安系統	網路及機房管理能力
5	網路安全管理能量	系統開發能力
6	系統操作能力	內部訓練及法規宣教
7	內部訓練制度	專業證照認證
8	專業證照認證	身分認證及權限管理
9	系統開發能力	備份及備援規劃與建立
10	人員安全評估	應變及復原機制
11	儲存媒體管理	入侵偵測防禦系統
12	機房維運	防毒控管及主機防毒
13	網路實體隔離	惡意名單阻擋及活動偵測
14	應變復原機制	憑證管理及認證
15	稽核程序	資安稽核與檢驗
16	存取控制規範	網路基礎設施
17	風險管理	資安事件管控及聯繫
18	使用者管理	保密傳輸裝備
19	防護管理	威脅弱點分析
20	資產風險評鑑	服務監控及告警
21		主機、網站及網段掃描
22		用戶虛擬主機安全隔離
23		資訊設備維護及管理
24		系統更新通知及管理
25		門禁設施及管制
26		設備產地與安全認證

資料來源：本研究整理

國防部於國軍雲端資料中心規劃指導中，已明確要求雲端資料中心網路、儲存設備及伺服器應採複式配置，以利單點失效時可由備援設備接替，並規劃第一階段同地區即時備援、第二階段跨地區異地快速備援機制及跨地區備份作業，且明訂各雲端資料中心管理權責，由各管理單位專責編組人員實施機房管理，另因應雲端架構資料集中儲存，將發展自動化資料加密機制，以確保雲端資料安全，故雲端資料中心在備份備援機制、保密傳輸裝備及門禁設施所得權重較低。

反觀雲端運算的導入，將對組織運用及資訊管理帶來相當程度衝擊，高階主管對於資訊安全應有相當程度的認知，才能支持資訊技術的採用，並要求共通性服務予以整併，避免軟硬體投資效益差及維運管理負擔。雲端資料中心儲存大量國防秘密與軍事機密，機房與系統管理者應審慎遴選，並強化人員考核，避免設備遭人為破壞及資料外洩。雲端資料中心為提高資訊服務的可靠度及確保戰時資訊系統的高存活率，應對系統操作及管理者，加強系統操作、故障排除及管理能力，降低人為錯誤。故兩者調查結果整體權重優先順序不同。

4.3 小結

依本研究調查結果，國軍雲端資料中心於建構資訊安全作為時，應首重「組織與人員專業能力」，持續培養專業人才，提升人員素質及落實考核制度，以確保運作安全無虞。

五、結論與建議

資訊資源向上集中及資訊機房整併為政府持續推動之政策，鑑於雲端運算及相關技術與標準漸趨完備，國防部依行政院指導規劃適用國軍特性之雲端資料中心，本研究透過德爾菲法實施專家意見調查，歸納出國軍建置雲端資料中心，應注意之資訊安全構面，再運用 AHP 建立國軍雲端資料中心資訊安全的評估指標權重，就研究過程及最後產生的結果，本論文結論與建議如下。

5.1 結論

本研究發現，主要構面權重以「組織與人員專業能力」占 35%比例最高，表示國軍在建置雲端資料中心時，專業人員認為組織制度及人員專業能力，將影響雲端運算是否能導入，人員素質是否能維持雲端資料中心持續及正常運作的關鍵因素，綜整結論如下：

一、雲端運算的特性就是以最少的管理人力，透過網路有效運用資訊及資源，提供使用者各項資訊服務；對國軍而言，以往由各軍種分散建置機房，因多次人力裁減，已逐漸面臨管理人力不足、運作效率欠佳及重覆投資等問題，機房整併及資訊人員集中，才能發揮人力及資源最大效能，使資訊服務有效支援任務遂行。

二、高階主管支持能使雲端技術在推動時，面對較少的困難和阻撓，使資安政策及要求能夠落實推展及執行，且雲端資料中心存有大量國防秘密與軍事機密，對於能夠存取機敏性資訊或賦予系統存取權限人員，應審慎評估適任性，避免肇生資料外洩或資安事件。

三、依本研究認知調查比對國軍資安事件肇生，的確多屬人為操作失當居多，加強人員系統操作、故障排除與管理能力，應可降低人為疏失；由於資訊科技發展快速，持續提升人員專業能力，以營運雲端資料中心所需之能力為依據，整體規劃訓練課程，提升人員的進階職能，以確保雲端資料中心運作能與時俱進，逐步強化資訊安全防護能力。

5.2 建議

根據前述之結果論述，本研究提出下列建議予國軍雲端資料中心的資訊安全管理者，或是資訊安全範疇內稽核主管與未來研究者：

一、本研究置重點於國軍雲端資料中心資訊安全探討，並非一般行政機關或企業進行個案驗證，後續可藉由本研究所獲得之結果，配合業務單位特性擬訂適用評估項目及準則。

二、定期召集高階主管及資訊人員辦理講習、教育訓練或研討會，強化資訊安全管控觀念，以利整體政策規劃、推動與通用性服務資訊系統整合，有效降低人力負擔及提

升運作效率。

三、針對可存取機敏性資訊、機房及系統管理人員，任職前應審慎評估適任性，並訂定嚴密審核制度,任職後定期實施安全查核及考核,避免遭惡意破壞及竊取機密資訊。

5.3 未來研究方向

本研究以德菲爾法實施專家意見調查，歸納及篩選國軍雲端資料中心資訊安全評估之指標，再運用層級分析法實施調查及分析，獲得指標整體權重，建議後續研究者未來研究方向如下：

一、運用因素分析法取代德菲爾法進行指標歸類及篩選，以提高調查結果之效度。

二、國軍雲端資料中心建置於與網際網路實體隔離之軍網，和其他行政機關或民間企業雲端資料中心（如行政院、中華電信、台灣大哥大等），所面臨的資安威脅不盡相同，並無法一體適用，可採用專家所建議的「政策」、「管理」及「技術」或其他構面實施探討，以周延資訊防護面向。

三、本研究主要採用層級分析法(AHP)，建立國軍雲端資料中心資訊安全評估指標之權重，對於類似主題可使用其他方法實施研究。

參考文獻

中華民國國家標準，2007。資訊技術－安全技術－資訊安全管理之作業規範（CNS 27002），經濟部標準檢驗局。

林麗娟，2011。建構企業導入雲端運算資訊架構評估指標，國立清華大學工業工程與工程管理學系碩士論文。

周宣光，2007。管理資訊系統-管理數位化公司（Management Information Systems: Managing the Digital Firm）七版，東華書局，台北。

國防報告書編纂委員會，2015。中華民國 104 年國防報告書，臺北：國防部。

國防總檢討編纂委員會，2017。中華民國 106 年四年期國防總檢討，臺北：國防部。

國防報告書編纂委員會，2017。中華民國 106 年國防報告書，臺北：國防部。

行政院，2017，行政院及所屬各機關資料中心設置作業要點。

林志章，2015，國軍網路作戰部隊作戰能力評估指標之研究，國防大學管理學院資訊管理研究所碩士論文。

吳世璋，2016。網路資料中心資訊安全防護能力評估指標之研究-以某國軍網路資料中心為例，國防大學管理學院資訊管理研究所碩士論文。

國防部，2011。國軍雲端服務發展計畫。

國防部，2015。國軍雲端資料中心規劃指導。

黃亮宇，1992。資訊安全規劃與管理，松崗電腦圖書公司，台北。

張博竣，2004。資訊安全管理實務，文魁資訊，台北。

張至伶，2011。企業導入雲端運用環境的資訊安全因素之研究，世新大學資訊管理學系碩士論文。

葉乃菁、李順仁，2004。網路安全理論與實務，文魁資訊，台北。

葉謦瑞，2014。企業導入虛擬化之資訊安全風險項目研究，中華大學資訊管理學系碩士論文。

劉國昌、劉國興，1995。資訊安全，儒林圖書有限公司，台北。

陳志誠、劉用貴，2016。建構雲端環境資料安全存取模型暨績效評估，中華民國資訊管理學報，第二十三卷，第一期：1-32 頁。

鄧振源，2002。計畫評估—方法與應用，海洋大學運籌規劃與管理研究中心，基隆。

鄧振源、曾國雄，1989。層級分析法的內涵特性與應用上，中國統計學報，第二十七卷，第六期：15-22 頁。

Chatterjee, D., Grewal, R., and Sambamurthy, V., 2002. Shaping up for E-commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies. MIS Quarterly (26:2), 65-89.

Choe, J. M., 1996. The Relationship Among Performance of Accounting Information Systems, Influence Factors, and Evolution Level of Information Systems. Journal of Management Information Systems (12:4), 35-39.

IBM, IBM Data Security Support Programs, USA, 1984.

ISO/IEC, ISO/IEC 27001:2013 Information Technology. Security Techniques. Information

Security Management Systems –Requirements, 2013.

Rusell, D. and Gangemi, G.T., 1992. Computer Security Basics. Califormia: O'Reilly & Associates Inc.

Saaty, T. L., 1980. The Analytic Hierarchy Process, 9th ed., New York: McGraw Hill.

Weill, P., and Olson, M. H., 1989, Managing Investment in Information Technology: Mini Case Examples and Implications. MIS Quarterly (13:1), 3-17.

iThome 電腦週刊，【2017 資安趨勢】資料外洩事件翻倍暴增，金融成竊資首選，參見 iThome 電腦週刊網站 https://www.ithome.com.tw/news/111218. [visited in 2017/12/18]。

iThome 電腦週刊，國發會建構首座政府雲端資料中心，加速政府各單位機房整併，參見 iThome 電腦週刊網站 https://www.ithome.com.tw/news/91866. [visited in 2017/12/18]。