中國文化大學資訊安全產業研發碩士班

碩士論文

Graduate Institute of R&D Master Program in Information Security Industry

Chinese Culture University

Master Thesis

雲端服務之個人資料保護與資訊安全治理：

根基於 ISO/IEC JTC 1/SC 27 之觀點

Personal Information Protection in Cloud Computing and Information Security Governance Base on View Point of ISO/IEC JTC 1/SC 27

指導教授：樊國楨 博士

Advisor: Kwo-Jean Farn, PhD

研究生：黃子恆

Andrew (Tzu-Heng) Huang

中華民國 100 年 5 月

May, 2011

中文摘要

論文名稱: 雲端服務之個人資料保護與資訊安全治理： 總頁數：96

根基於 ISO/IEC JTC 1/SC 27 之觀點

校(院)所組別: 中國文化大學資訊安全產業研發碩士專班

畢業時間及題要別: 九十九年度第二學期碩士學位論文提要

研究生:黃子恆 指導教授: 樊國楨 博士

論文提要內容:

由於資訊安全議題是需要定期的維護及探討，使這些要求及規範達到其可用性、有效性、及完整性，國際標準(ISO)ISO/IEC JTC 1/SC 27各工作小組(Working Group)每六個月輪流在51個會員國家開會探討，本論文利用SC 27小組開會所提出的觀點，ISO/IEC JTC 1/SC27 N9001 和 ISO/IEC JTC 1/SC 27 N117來探討資訊安全治理之議題，ISO/IEC JTC 1/SC27 N8808 和 ISO/IEC JTC 1/SC27 N9226 探討個人資料之保護，由於資訊系統日益的變化，雲端運算之發展已勢不可當，企業或組織已被迫正式面對雲端運算上的各項資訊安全問題，由資訊安全治理到個人資料保護ISO/IEC JTC 1/SC27 已發文各會員針對雲端運算進行討論，ISO/IEC JTC 1/SC27 N9314 針對中小型企業於雲端運算的觀點做出了調查，

並提出雲端技術對資訊安全的好處、存在風險、及資訊保證架構，由PCI DSS對ISO 27001標準做補充對雲端提供商及外包商提出控制措施建議。本論文根據ISO/IEC JTC 1/SC27 WG1和WG5所提出之文件來探討雲端運算於個人資料保護及資訊安全治理，並對其相關安全措施提出適當的建議。

關鍵字: 資訊安全管理系統、資訊安全治理、個人資料保護、雲端運算

英文摘要

Personal Information Protection in Cloud Computing and Information Security Governance Base on View Point of ISO/IEC JTC 1/SC 27

Student: Andrew (Tzu-Heng) Huang Advisor: Prof .Kwo-Jean Farn

Chinese Culture University

ABSTRACT

Information security requirement is necessary to maintain and discuss, which allow those requirements to reach availability, efficiency, integrity. Working groups in International Standard Organization ISO/IEC JTC 1/SC 27 will have meeting in 51different countries every 6 month. This these utilize ISO/IEC JTC 1/SC27 N9001 and ISO/IEC JTC 1/SC 27 N117 to discuss Information security governance, and use ISO/IEC JTC 1/SC27 N8808 and ISO/IEC JTC 1/SC27 N9226 to discuss Personal information security. Moreover, the information system is getting changed everyday, company or organizations has to be accept cloud computing is inevitably when face information security issues. ISO/IEC JTC 1/SC 27 has issued ISO/IEC JTC 1/SC27 N9314 to allow members to discuss SME perspective on cloud computing. Also has recommended the benefit, risk, and information assurance architechture of cloud computing in information security.Also ISO 27001 by the PCI DSS standards for the supplement of cloud providers andoutsourcing companies to provide recommendations for control measures.This these base on ISO / IEC JTC 1/SC27 WG1 and WG5 documents to discuss cloud computing on personal information protection and information security governance, and its associated security controls to make appropriatere commendations.

Keywords：ISMS、ISG、Personal information protection、Cloud computing

誌謝詞

本論文得以順利完成，首要感謝指導教授樊國楨老師耐心的指導，由於老師的嚴謹、細心才能順利完成。同時，也要感謝口試委員梁德昭教授和蔡敦仁所長對於論文的指導，給予精闢的見解與意見，使我的論文更臻完備與嚴謹，感激並銘記在心。

兩年忙碌的碩士班生活，承蒙所上老師、專員、班上同學照顧，在此感謝佳蓉、育芸、彥如等大力幫忙；也感謝同事及主管的協助，在此要感謝陳宗光總經理、郭明茂協理。特別也要感謝家人的全力支援，使我順利完成研究所的學業；在此致上我最高的謝意。

黃子恆
謹識於中國文化大學資訊安全產業研發碩士班
中華民國一百年五月

目錄

表目錄

圖目錄

第一章 緒論

第一節 研究背景

隨著個人資料保護法在2010年5月26日之公布，個人資料保護的資訊安全管理議題已成為眾所矚目之焦點；根基於此，本論文以國際標準化組織(International Organization for Standardization，簡稱ISO)制定已頒布與進行中的資訊安全管理系統(Information Security Management System，簡稱ISMS)標準之組織ISO/IEC JTC 1/SC27觀點為核心，探討並提出合規於個人資料保護之ISMS標準化以及擴增控制措施實作的方法並與資訊安全治理之間的關係提出看法。

近年來，政府機關、學校單位、醫療機構、金融/電信/高科技產業均相當重視資訊安全管理系統(ISMS)，截至 2011 年 2 月止，全球通過 ISO 27001 認證單位數已超過 7136 個，台灣有 410 個單位(包括公民營單位)排名全球第五名，僅次於日本 3790 個、印度 516 個、中國 495 個、英國 460 個，如表 1-1 所示。

ISO 27001 各國驗證數：

表 1-1 ISO 27001 各國驗證數

Japan	3790	Slovenia	17	Macau	3
India	516	Philippines	15	Morocco	3
China	495	Netherlands	14	Argentina	2
UK	460	Pakistan	14	Belgium	2
Taiwan	410	Vietnam	14	Bosnia Herzegovina	2
Germany	154	Iceland	13	Cyprus	2
Korea	106	Saudi Arabia	13	Isle of Man	2
Czech Republic	101	Indonesia	11	Kazakhstan	2
USA	99	Kuwait	11	Macedonia	2
Hungary	72	Portugal	10	Ukraine	2
Spain	67	Russian Federation	10	Armenia	1
Italy	64	Colombia	9	Bangladesh	1
Poland	58	Iran	9	Belarus	1
Malaysia	52	Norway	9	Denmark	1
Austria	37	Sweden	9	Ecuador	1
Ireland	37	Bahrain	8	Jersey	1
Thailand	37	Switzerland	7	Kyrgyzstan	1
Romania	34	Croatia	7	Lebanon	1
Hong Kong	33	Canada	6	Luxembourg	1
Greece	30	Oman	5	Malta	1

Australia	29	Peru	5	Mauritius	1
Singapore	29	South Africa	5	Moldova	1
Mexico	24	Sri Lanka	5	New Zealand	1
Brazil	23	Dominican Republic	4	Sudan	1
Slovakia	23	Egypt	4	Uruguay	1
Turkey	22	Lithuania	4	Yemen	1
UAE	20	Qatar	4		
France	19	Chile	3		
Bulgaria	18	Gibraltar	3	**Total**	**7136**

資料來源：International Register of ISMS Certificates http://www.iso27001certificates.com/Register%20Search.htm（2011/5/20）

反觀台灣為世界排名第五名，但在日常生活中企業與消費者間時常出現資訊安全的漏洞，刑事警察局犯罪預防科指出，Yahoo 奇摩與 PChome 兩個網購平台，每週至少外洩百筆個資。刑事警察局犯罪預防科指出，165 反詐騙諮詢專線至 2009 年一月總共接獲了 2 萬 5 千 146 件詐騙投訴電話，排名第一的是個人資料外洩詐騙事件，件數達 8 千 865 件，占總數的 35%，未收到網購產品的詐騙事件則名列第二，件數為 8 千 476 件(My USB ONLY 警方：Yahoo 奇摩與 PChome 成個資外洩幫兇 http://www.myusbonly.com/usb-security-device-control/news_read.php?id=263,2011/5/20)。

因近年來各大型企業紛紛朝向雲端運算架構開始發展，就雲端運算安全架構及規範都還沒有明確的規定，「CNNIC 分析師王常青認為，雲端運算安全至少包含兩個層面的問題：一是雲端運算環境下，應用程式和關鍵資料對用戶完全透明，應如何保證它們不被病毒或非法程式攻擊？二是雲端運算提供商的中立和公信力問題—企業能否將自己核心資訊資源託付給一個第三方？」(http://smb.chinabyte.com/314/11362814.shtml,2011,5,20)

所以本研究於雲端運算之個人資料保護與資訊安全治理之間之探討是具有相當的必要性。

第二節 研究目的

本論文以國際標準化組織(International Organization for Standardization，簡稱ISO)制定已頒布與進行中的資訊安全管理系統(Information Security Management System，簡稱ISMS)標準之ISO/IEC JTC 1/SC27組織的觀點為核心，利用WG1和 WG5進行中之文件來探討雲端運算之個人資料保護與資訊安全治理，Sony近日被駭客攻擊而導致龐大的客戶資料外洩，造成公司嚴重的損失，本論文將對雲端運算的個人資料保護及資訊安全治理

相關安全措施提出適當的建議。

第三節 研究範圍

本研究根基於 ISO/IEC JTC 1/SC27 之觀點分別就資訊安全治理及個人資料保護提出討論，於個人資料外洩相關案例作研究，利用 ISO/IEC JTC 1/SC275 之相關文件分析個案例中違反之項目影響之結果，並因雲端運算主要的安全議題為個人資料隱私和第三方及外包，將於案例探討中對 Sony 被駭客盜走個人資料案例以 ISO/IEC JTC 1/SC 27 N9314 提出雲端風險分析，與參考支付卡行業之標準補齊 ISO/IEC27001 於此項之不足 ，對雲端運算提出第三方及外包規範應用之建議。

第四節 研究流程及方法

4.1 研究流程

確立研究動機與目的進而蒐集相關文獻理論探討及研究主題與範圍確認以界定研究主題與研究架構。其後再蒐集個資案外

洩案例之案例加以分析。將資料彙整並以 ISO/IEC JTC1/SC27 之研究內容加以討論出看法，研究流程如圖 1-1 所示。

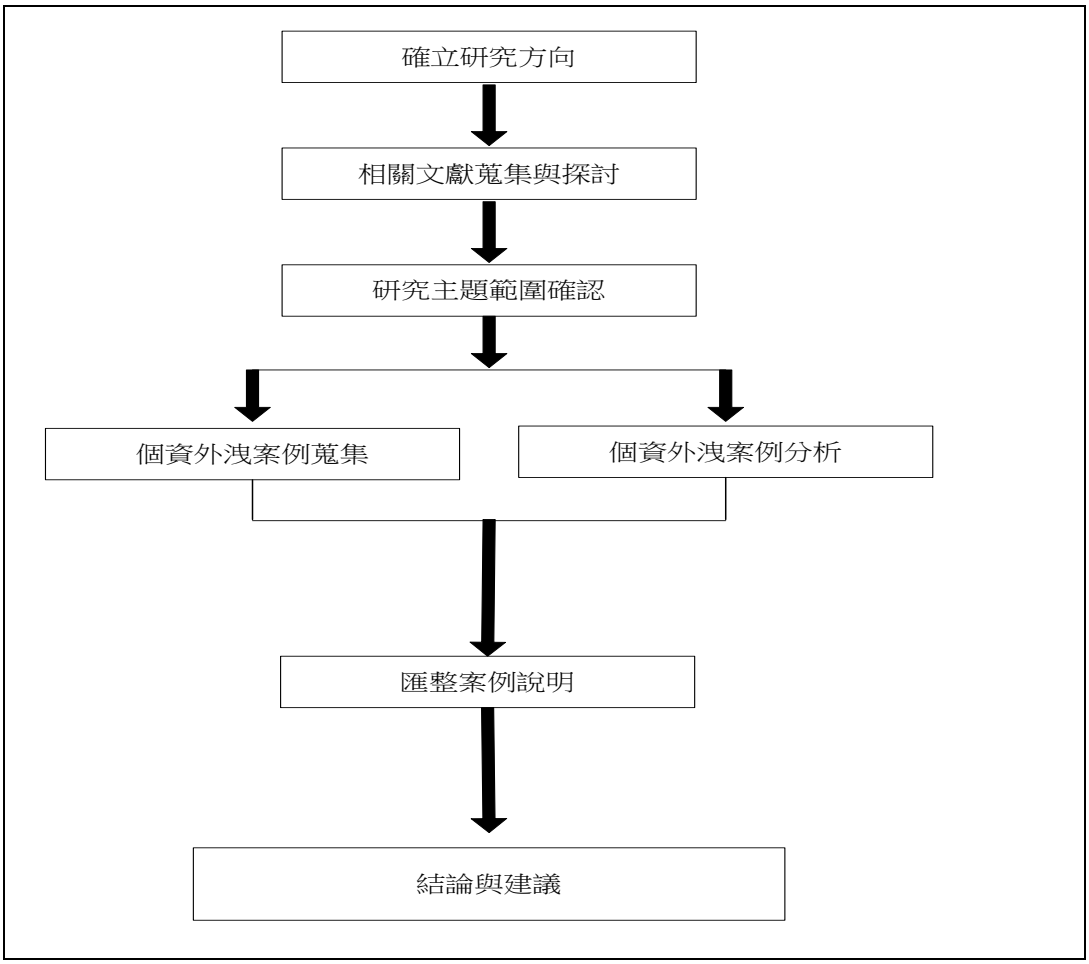


圖 1-1 研究流程

資料來源：本研究

4.2 研究方法

個案研究法:

(case study)對於一個或多個個人、團體、社群、企業或機構之

背景、現況、環境和發展歷程予以觀察、記錄、分析，就其內部和外部的諸種影響而言得出某些階段性的變化模式來。

1. 使用多種收集資料方法。
2. 分析收集的對象可能是單一或是多個實體，例如，群體、組織、人。
3. 針對每一個實體進行瞭解與其複雜性。
4. 個案研究法不僅可用在探索性階段與分類性研究和命題或假設提出，也可以使用在敘述性和解釋性階段。
5. 在檢視單一或多個環境、組織或群體時，沒有實驗設計、變數操弄或控制。
6. 研究目前的現象，解決目前的問題。
7. 如何或為何做的問題適合用在個案研究中，可以在未來中作為相關研究的基礎。
8. 個案研究的最後結果跟研究者的分析、整合能力有相當大的關係。
9. 針對不同的研究對象與使用不同的資料收集方式可以發展一些新的假說。
10. 個案研究法不預設哪些是依變數及研究變數。

內容分析法:

內容分析法是對相關理論的資訊作客觀性與系統性的推理，為非干預性的研究，主要是研究者針對不同的事物、溝通形式進行研究，以客觀且系統的態度，對文件內容進行分析研究，藉以推論文件的內容的意義與環境背景，主要的範圍是新聞報導、網站、書籍、影片、報紙、電視、會議紀錄等。

第二章　文獻探討

文獻探討部份分為四節，第一節探討 ISO/IEC 27001 的進化流程與 ISO/IEC JTC1/SC27 之間的關係；第二節主要是探討資訊安全治理與 ISMS，與其框架及新的觀點；第三節則為個人資料保護與 ISMS;第四節為 ISO/IEC JTC 1/SC27 對雲端運算之觀點。

。

第一節　ISO/IEC 27001 之進化流程

國際標準化組織(International Organization for Standardization，簡稱ISO)技術管理委員會(Technical Management Board，簡稱TMB)為求索管理系統要求事項之一致性，於2001年先行出版ISO Guide 72 (Guidelinesfor the justification and development of management system standards)作為準備，並於2008-06~2010-12以能源管理(Energy Management)為標的試行。自2006年起組建管理系統標準(Management System Standards, MSS)之策略顧問群(Strategic Advisory Group，簡稱SAG-MSS)，要求其第13技術顧問群

(Technical Advisory Group，簡稱TAG)亦即JTCG (Joint Technical Co-ordination Group)發展各個管理系統之共同觀點(Joint Vision)並校準現有的MSS與任一新MSS，如圖2-1。

1. JTCG 於2008 年完成草案後，在2009-04-10提出MSS之建議書：ISO/TMB/TAG13-JTCG/TG3/N034，請各個相關之技術委員會等審查，期能在2010年完成MSS。
2. 2009-04-23，ISO/IEC JTC1/SC27以N7616號文件轉發MSS之建議書。
3. JTCG於2010-05-17提出MSS之草案：JTCG/TF1/N28&JTCG/TF3/N086，請各個標準化機構研究並提供意見(Study and comment)。
4. ISO/IEC JTC1/SC27於2010-07-15提出：「ISO/IEC 27001與MSS前景白皮書(WHITEPAPER FUTURE OF ISO/IEC 27001 AND MANAGEMENT SYSTEM STANDARDS (MSS))」。
5. ISO/IEC JTC1/SC27遵循MSS之「高階管理系統結構以及一致性文句與共同名詞(Draft high level management system structure with draft identical text and common terminology)」，於2010-11-15公布ISO/IEC 4th WD 27001

新版。資料來源：ISO/IEC JTC1/SC27 N7616:2009-04-23

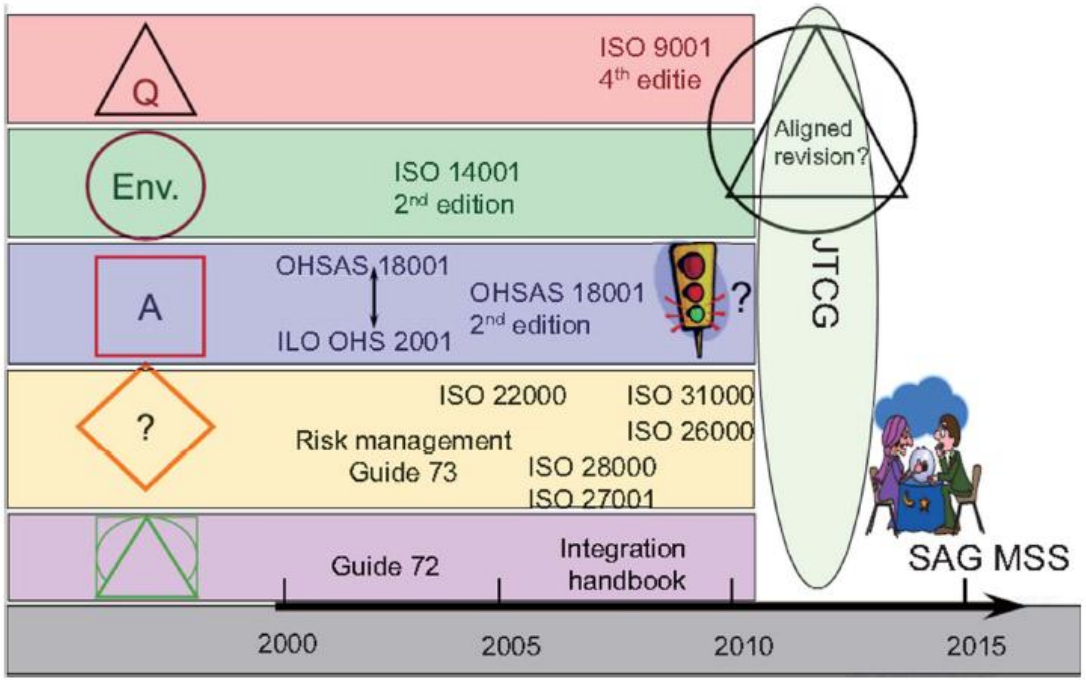


圖 2-1 管理系統之效準

資料來源: Waumans, R (2010) JTCG Introduction, Buenos Aires, May 2010

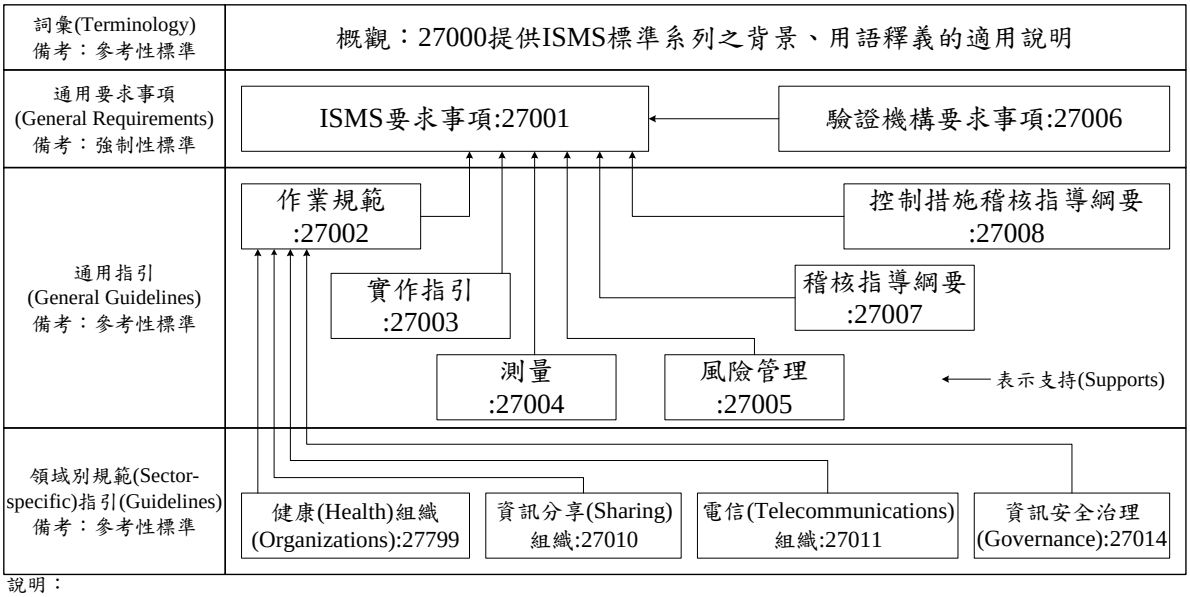
目前 SC 27 各工作小組(Working Group,WG)每六個月輪流在 51 個會員國家，召開一次為期一週之工作小組會議。而 SC 27 本身則在每年的春天，結合當年第一次之工作小組會議，召開為期兩天之大會。

SC27 的工作範圍中，與資訊安全管理系統(Information Security Management System,ISMS)相關的標準工作主要橫跨

WG1 及 WG5 如圖 2-3。目前 ISO/IEC JTC1/SC27/WG1 的主要工作範圍是發展資訊安全管理系統(ISMS)的標準與指引，具體的來說這包括 ISO/IEC 27001 ISMS 標準系列(此系列的標準包括了 27001~27006)的發展與維護，和有特定需求及發展 ISMS 指引的組織及委員會協調合作 (Liaison)，目前已建立合作關係的包括電信領域的 ITU-T、健康醫療領域的 TC 215、金融服務領域的 TC 68 及汽車產業。除此之外，WG1 也正在與交通領域的 TC 204 及博奕領域的世界彩票協會(World Lottery Association)建立合作關係。WG1 已發展及正在發展中的標準包括，如圖 2-2：

- ISO/IEC 27000 – Overview and vocabulary(Final Committeee Draft)
- ISO/IEC 27001:2006 – ISMS requirements
- ISO/IEC 27002:2005 – Code of practice for information security management
- ISO/IEC 27003 – ISMS implementation guidance (Final Draft International Standard)
- ISO/IEC 27004 – Information security management measurements(Final Committeee Draft)

- ISO/IEC 27005:2008 - Information security risk management
- ISO/IEC 27006:2007 - Accreditation requirements
- ISO/IEC 27007 - ISMS auditing guidance (Working Draft)
- ISO/IEC 27008 - Guidance for auditors on ISMS controls
- ISO/IEC 27011:2008 (ITU-T X.1051) - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27014 - Information security governance framework



說明：
1.資料來源：ISO/IEC 27000:2009-05-01，頁12，圖1；與本研究。
2.備考：ISO/IEC 27001、ISO/IEC 27005均參照ISO 31000等修正中，預定於2012年5月完成。
3.參考資料：2nd Working document for revision of ISO/IEC 27000, ISO/IEC JTC 1/SC 27 N9027, Page 15, Figure 1, 2010-11-23.

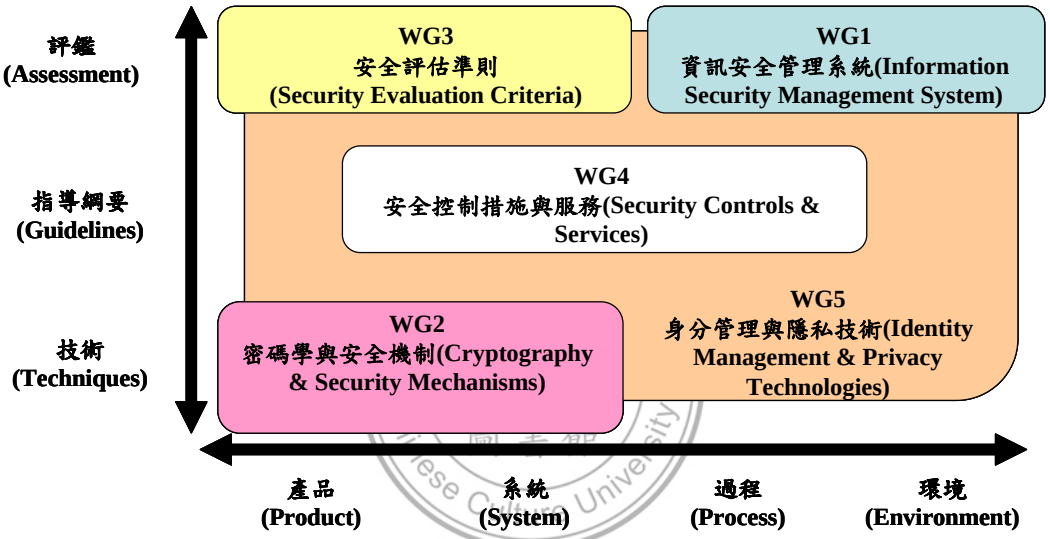
圖 2-2 ISMS 標準系列框架

資料來源:ISO/IEC 27000:2009-05-01，頁 12，圖 1

此外由於在 ISO/IEC 27006 的標準中，已經帶出了資訊安全管理系統控制措施之技術確認(Technical Verification)需求(27006 Annex D)，然而目前大多數之稽核僅做到文件檢視，同時稽核員也並不一定具備技術稽核之能力，因此 WG 1 於 27008 控制措施稽核指導綱要內已提出技術稽核作法，研究標的主要包括了瑞典及日本兩國所進行的技術稽核作法。

目前 ISO/IEC 27001 系列標準除 27007 目前還在工作小組草擬階段外，其他都已進入最終委員會草案(Final committee draft,

FCD)或最終國際標準草案(Final Draft International Standard, FDIS)，因此很快應當就會陸續正式公布，代表 27001 系列的標準已漸趨成熟。由 WG 1 目前的發展來看，27001 系列的標準現階段之工作計畫將偏重技術稽核的作法及特定產業之實作指引。



資料來源：1. Walter Fumy (2005) ISO/IEC JTC1 Plenary Meeting – Banff, Canada – November, 2005。
2. http://www2.ni.din.de/ (2006-08-02)。
3. 本研究。

圖 2-3 ISO/IEC 安全標準工作框架調整現況(2005 年 5 月之後)

資料來源:Walter Fumy(2005) ISO/IEC JTC1 Penary Meeting-Banff, Canada-November, 2005.

WG 1 目前也正在進行新的研究項目及專案建議，包括：

- 資訊安全治理（Information security governance)。

- 特定產業之資訊安全管理體系標準－世界彩券協會(Sector-Specific ISMS Standards for the World Lottery Association)。
- 資訊安全管理：跨政府與產業交互影響及交流(Information security management: sector to sector interworking and communications for industry and government)。
- 特定產業之資訊安全指引－關鍵基礎建設(Information security for Critical Infrastructure － Sector-specific guidance)。
- 電子化政府資訊安全管理指引（ISM guidelines for e-government services)。
- 稽核員資訊安全管理控制(Guidance for auditors on ISMS controls)。

在上述研究項目中，跨政府與產業交互影響及交流及關鍵基礎建設資訊安全指引具有高度的相互關聯性。跨政府與產業交互影響及交流之研究是希望未來能有國際標準提供相同企業及組織在產業內部、跨產業及與政府部門間交互影響及交流之指引。預期

此標準會針對危機及承平時刻關鍵基礎建設之保護，以及在一般商業情境因為交互影響如何相互認可，以滿足法律、法規及合約之義務提出指引說明。目前跨政府與產業交互影響及交流標準目前規劃將包含五大部分，我們可看出在 Part 3 中特別將關鍵基礎建設中相當重要之工業控制單元：系統監控和資料擷取系統(Supervisor Control And Data Acqusition,SCADA)之流程管理及控制措施納入：

- Part 1：概論、塑模及原則(Overview, model and principles)。
- Part 2：交互影響及交流政策(Interworking and communications policy)。
- Part 3：流程管理及控制措施，包括系統監控和資料擷取系統(Process management and control, which includees work on SCADA)。
- Part 4：危機管理協定(Crisis management procotol)。
- Part 5：資訊安全管理之經濟制度(Economies of Information security management)。

第二節　ISMS 與資訊安全治理

2.1 資訊安全治理定義及框架

(1)治理(Govern)(動詞):管理國家、組織或人的政策和事務。(conduct the policy and affairs of a state, organization, or people)(ISO，2010)。

(2)治理(Governance)(名詞):治理的行動或方法(the action or method of governing)(ISO/IEC 38500:2008)。

(3)公司治理 (Corporate governance):主持管理與控制組織之系統(the system by which organizations are directed and controlled.)。(採自 Cadbury 1992 與 OECD 1999)(ISO/IEC 38500:2008)

(4)IT 治理(IT governance):主持管理與控制在現在及未來使用 IT 之系統。(the action or method of governing IT, The

system by which the current and future use of IT is directed and controlled.)(ISO/IEC 38500:2008)

IT Governance Institute 指出 IT 治理是公司治理(Corporate Governance)的一部份，並非獨立的活動。它由領導階層，組織架構與程序所組成，其目的在於確保 IT 能維持並擴展組織相關的策略或期望。並透過發展與維持有效的 IT 控制、責任歸屬、績效管理與風險管理，來創造最大的商業價值。

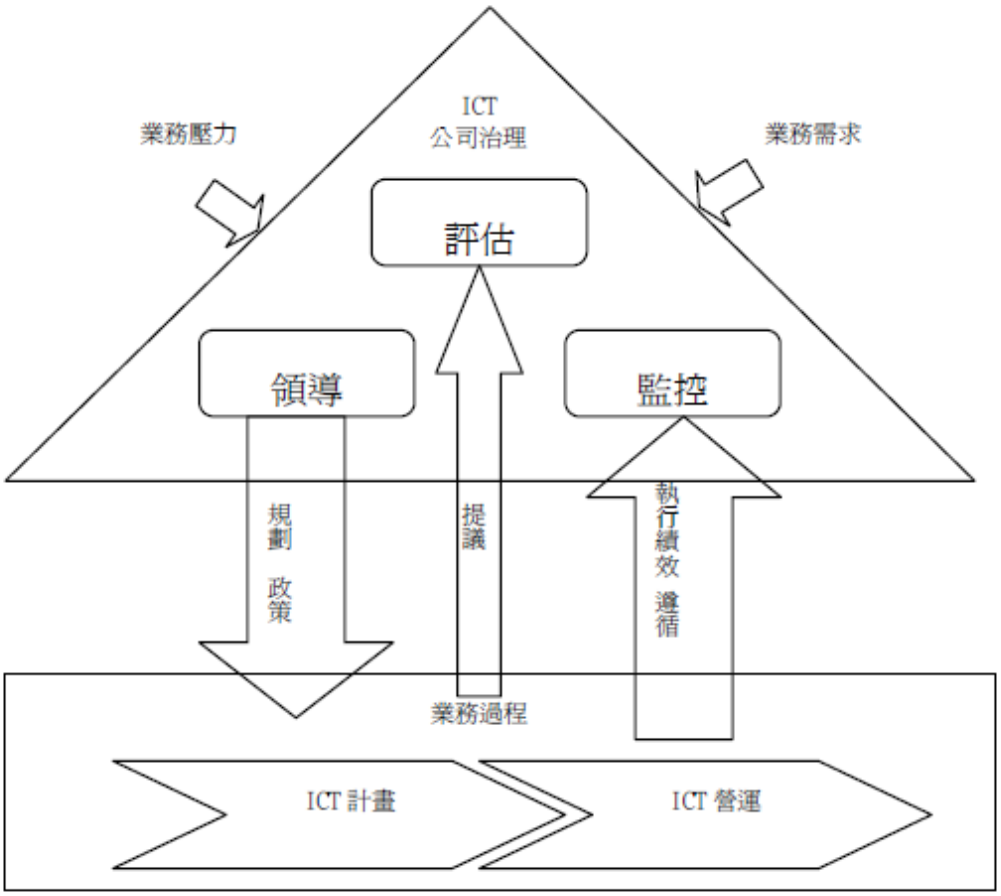


圖 2-4　IT 治理之架構圖

資料來源:ISO/IEC 38500 資訊技術之公司治理，頁 15，圖 1

(5)資訊安全治理(Information Security Governance)：透過幫助達到用經營目標的資訊安全性活動的戰略性結盟的一種公司治理的不可缺少的要素，分派責任和決策能力，且遵守有關的法律法規。資訊安全性的活動被指導並且控制的系統 (an integral element of Corporate governance by helping to achieve strategic alignment of information security activities with business objectives, assign responsibility and decision making capability, and comply with related laws and regulations. The system by which the activities of information security is directed and controlled.) (ISO/IEC 3rd WD 27014)。

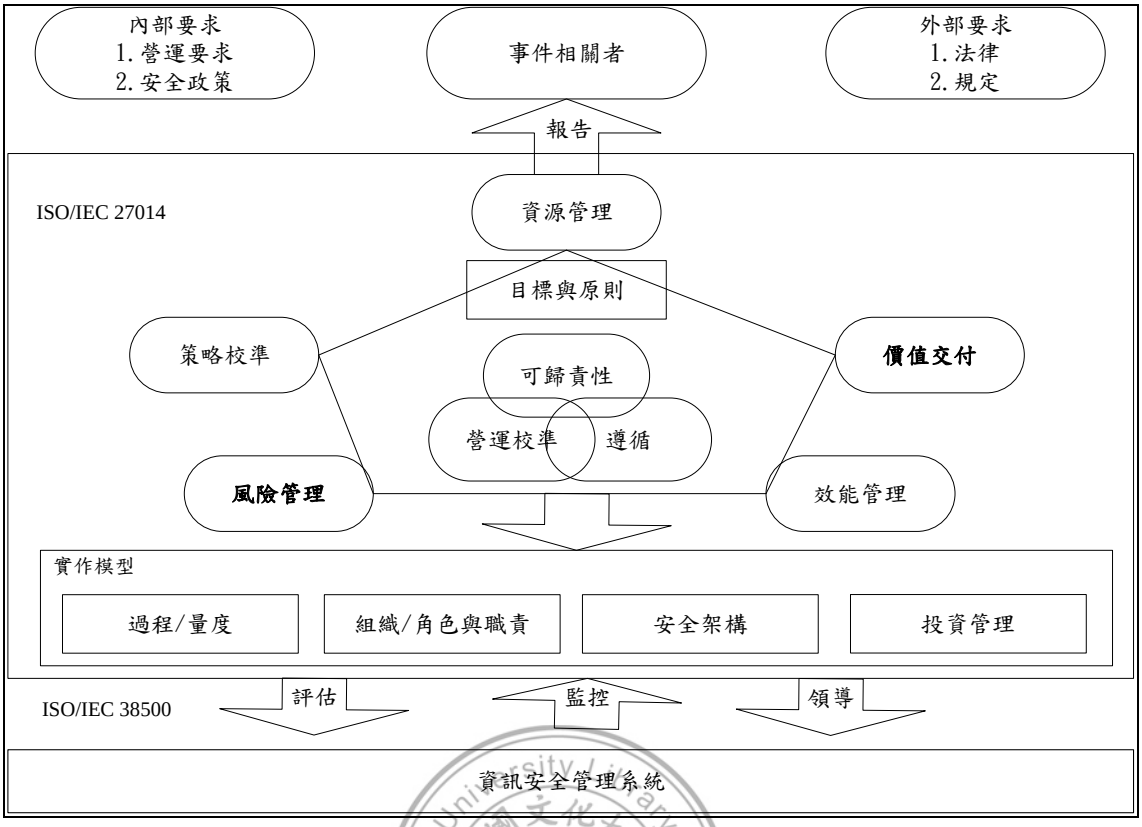


圖 2-5 ISO/IEC 3rd WD 27014 資訊安全治理框架

資料來源: ISO/IEC 3rd WD 27014，與本研究

資訊安全治理是一種藉由資訊安全系統(含資訊安全技術應用與資訊安全管理)的運作，從風險管理的角度，落實個人資料保護，並提昇整體資訊安全績效與落實資訊安全自律及自我調適的管理過程。除此之外，資訊安全治理在運作上需考量內、外部環境如圖 2-5，從治理及管理兩層面，明確規範相關人員之權責分工。

在內部環境需考量營運要求、安全政策等因素；外在環境需考量法律、規定等因素。

而有效的資訊安全治理需分為兩個層面進行：治理(Governance)層面與管理(Management)層面

- 治理層面

  包括組織議題與法律／規章。董事會與高階主管應為組織設立資訊安全的願景(Vision)、策略(Strategy)與使命(Mission)。並透過指揮(Directing)產出資訊安全政策(Policy)，以顯現對組織資訊安全的承諾與支援；透過控制(Controlling)活動來確保資訊安全計畫執行的有效性。

- 管理層面

  包括資訊科技的基礎建設、資訊安全風險／績效、標準／最佳實務等。執行團隊應依據資訊安全政策(Policy)進行資訊安全的建置(Implement)與管理(Manage)，並定期回報(Reporting)落實情形；高階主管則須依據回報情形，透過指揮與控制持續改進，以確保資訊安全政策的適當性與有效性。

2.2 ISO/IEC JTC 1/SC 27 及資訊安全治理

ISO/IEC JTC 1/SC 27/WG 1 於 2010 年 11 月 15 日提出第四次的工作草案，內容裡提出管理系統標準適用於 ISO/IEC 27001 要求事項，其章節如下:

第 1 章：適用範圍(Scope)。

第 2 章：引用標準(Normative references)。

第 3 章：用語釋義(Terms and definitions)。

第 4 章：組織全景(Context of the organization)。

第 5 章：統禦力(Leadership)。

第 6 章：規劃(Planning)。

第 7 章：支援(Support)。

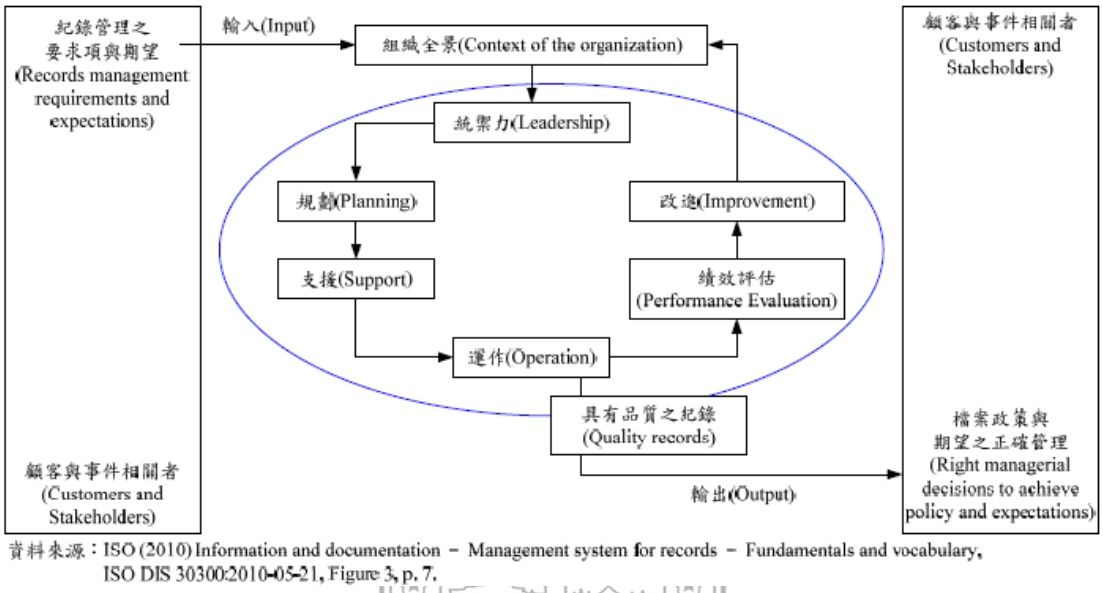
第 8 章：運作(Operations)。

第 9 章：績效評估(Performance evaluation)。

第 10 章：改進(Improvement)。

資料來源：：ISO/IEC JTC1/SC27 N7616:2009-04-23，附錄 B。

於 MMS 中，以目前列為所有管理系統基礎之記錄管理系統為例，過程管理的塑模如圖 2-6 所示:



資料來源：ISO (2010) Information and documentation – Management system for records – Fundamentals and vocabulary, ISO DIS 30300:2010-05-21, Figure 3, p. 7.

圖 2-6 過程式之管理系統紀錄管理模型(Process-based MSR model)

資料來源:ISO(2010)Information and documentation- Management system for records –Fundamentals and vocabulary, ISO DIS 30300:2010-05-21 Figure 3, p.7.

欲推動 ISMS 更加的完整化，ISO/IEC JTC1/SC27 N9001:2010-11-05 於第五章及第七章分別提到了統禦力及支援，在 PDCA 循環模型 (Plan-Do-Check-Act Model)前後分別加上了統御力及支援使該模型更加的完整，欲推行 ISMS 並不是只

有中階管理層和員工的工作，在資訊安全治理方面更需注重於高階主管的規範。

統禦力裡提及最高管理者應展現其承諾確保資訊安全管理系統，與該組織的戰略方向兼容，整合資訊安全管理系統的要求納入本組織的業務流程，提供資源，去建立、實施、保持並不斷改進資訊安全管理系統，持續加強宣導有效的資訊安全管理的重要性，和持續確認各項資訊安全管理系統的要求，確保資訊安全管理系統達到其預期成果，及持續增進指導和支援。

最高管理者必須應建立一個資訊安全政策，對該組織的宗旨是最適當的，提供設置資訊安全目標框架，承諾持續改進資訊安全管理系統。最高管理者應分配責任和權力來，向高層管理人員報告資訊安全管理系統的績效，及確保資訊安全管理系統符合 ISO/IEC 27001 的要求。

支援裡更表述了組織在推動資訊安全管理系統時應注意的表現，應提供充足的資源，確保資訊安全程序支援業務的要求;正確的應用所有實施的管制來保持資訊足夠的安全。全球傳統的資訊安全平均花費大約限制在 IT 總預算的 3% 到 5%(http://www.microsoft.com/business/smb/zh-hk/security

/planning-security-budget.mspx, 2011/5/20)，大多分配到的資源相當的少，所以在 ISO/IEC JTC1/SC27 N9001:2010-11-05 第七章裡特別規範了應給予資訊安全適當的資源。

確保具備必要能力的人在組織控制下工作否則會影響其資訊安全的效能，確保員工有足夠的能力且基本上有適當的教育，培訓和經驗，在適用情況下，採取行動，以獲得必要的能力，並評估所採取的行動的有效性，行動可能包括，例如：提供培訓，師徒制，或重新分配現有的員工，或僱用或外包有資格的廠商。

於文件部分支援提到資訊安全管理系統文件應包括管理決策的記錄，並確保可以追溯到管理決策和政策，並確保所記錄的結果是可重複。

建立和更新記錄資料確保其適當：

-識別和描述（如標題，日期，作者，數量）

-格式（如語言，軟件版本，圖形）和媒體（如：紙張，電子版）

-審查和批准其正確性

資訊安全管理系統的文件化資訊應予以控制:

-分佈(distribution)

-獲取(access)

-儲存和保存(storage and preservation)

-取回和使用(retrieval and use)

-控制換版(control of change e.g. version control)

-保持易讀性（即清晰閱讀）(preservation of legibility)

-防止誤用過時的資訊(prevention of the unintended use of obsolete information)

-保留和處置(retention and disposition)

第三節ISMS與個人資料保護

3.1 ISO/IEC 27001探討

ISO27001 資訊技術-安全技術-資訊安全管理系統-要求事項「Information Security Management System (ISMS) - Requirement」,是目前國際上最廣泛有效的管理制定標準來確保資訊系統安全與持續運作，為整體資訊安全做一個良好起點與規範及系統化的方法。用以建立、執行、檢核、改善資訊安全管理系統(Information Security Management System, ISMS) 之模型。此標準規範目的是在整體系統建構和管理制度面上時，忽略安全面的考量,藉由內部稽核、外部稽核、資訊安全事件的回報、

審查機制，已達到預防資訊安全造成危害的風險或降低損害風險達到可以接受的範圍之內。

ISO27001 資訊安全國際標準前身是 BS7799，BS7799 是國際資訊安全稽核規範，由英國標準協會在 1995 年提出、修改，已被國際標準化組織接納為國際標準規範，簡稱 ISO。BS7799 主要分為 BS7799-1 與 BS7799-2。表 2-1 為英國標準、國際標準、台灣標準比較表：

表 2-1 英國標準、國際標準、台灣標準比較表

英國標準	國際標準	台灣標準比較表
BS7799-2	ISO 27001：2005(E)(資訊安全管理系統要求事項)	CNS 27001（2007 年修訂公布）
BS7799-1	ISO 27002: 2005(E)(資訊安全管理之作業規範	CNS 27002（2007 年出版）
	ISO 27003: 2010(E)(資訊安全管理系統	CNS 27003（2011 年 7 月已完成草案),

	實作指引) ISO 27004: 2009(E) (資訊安全管理量度 (Metrics)與測量)	CNS 27004(2011 年 5 月已完成草案)
BS7799-3	ISO 27005: 2011(E) (資訊安全風險管理)	CNS 27005(2010 年 2 月出版)
	ISO27006: 2007(E) (稽核與驗證機構要求)	CNS 27006(2010 年 2 月出版)

資料來源:ISMS 建制實務(二)風險管理，ISO/IEC JTC1/SC27 (IT Security Techniques) Chairman, Mr. Walter Fumy, 2004-10-04。

ISO/IEC 27002:2005(BS7799-1)主要為參考文件，提供廣泛性的安全控制措施作為現行資訊安全最佳作業方法，其中包含 11 個領域、39 個控制目標與 133 個控制事項，但這些是不作為評鑑與驗證標準。根基於 BS7799-2 ISO 公佈 ISO27001:2005 資訊安全管理系統國際標準，台灣標准為 CNS27001(2006 發行)，此標準為資訊安全管理系統(ISMS)，建立實施與書面化之具體要

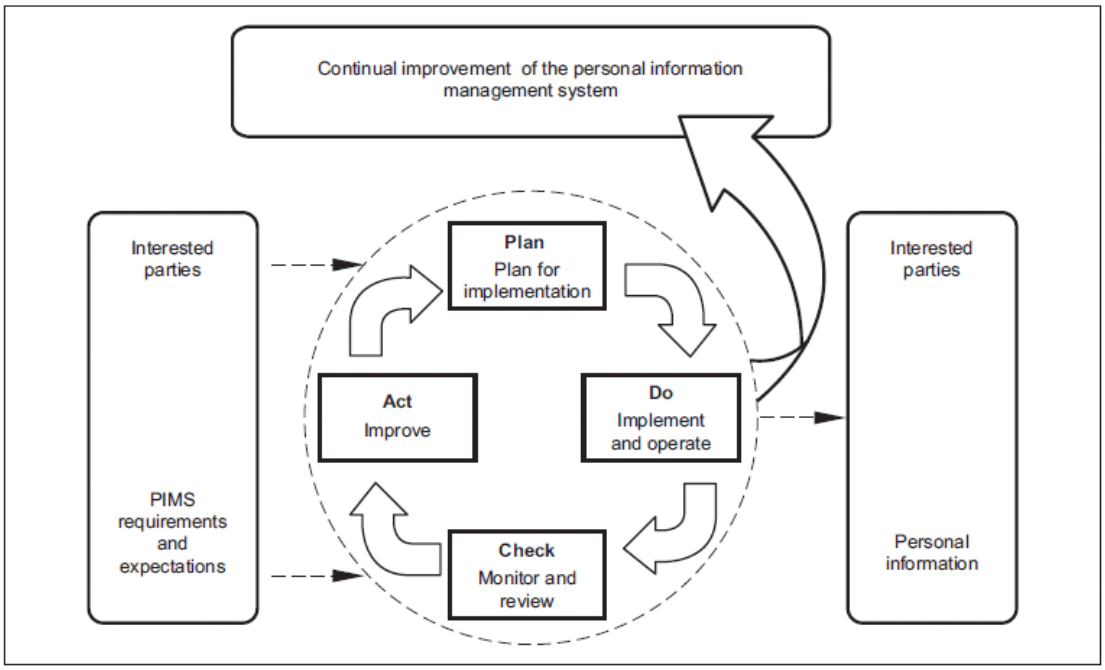
求，依造組織的需求，規定實施安全控制措施的要求，同時用來驗證與評鑑的標準。

ISO27001 精神是希望組織從上到下都能達到合乎資訊安全目的，依據該單位的資訊安全政策、目標、型態、規模、需求、資源、業務性質等特性：在資訊安全範圍內資訊資產進行風險評估與風險評鑑，針對高風險資產對應 ISO/IEC 27001 控制項與控制措施進行風險管理，根據相關法律規定、法規及即訂合約的要求，適當評估風險及對應措施後擬定一份組織適用性聲明書，依序進行 PDCA 循環模型進行持續有效的風險管理。ISO/IEC 27001 所表示之資訊安全管理的作法導向，讓使用者得知下列事項的重要性：

- 得知組織所需要的資訊安全需求，以及瞭解建立資訊安全政策與目標的需求。
- 在組織整體營運過程風險之中，落實各項控制措施的實作及運作進而降低組織的資訊安全風險。
- 監控與審查 ISMS 落實之績效及有效性。
- 憑著客觀的角度持續改進。

- 這標準使用建立、執行、檢核、改善(Plan-Do-Check-Act, PDCA)管理循環模式。

所謂「資訊安全管理系統」，是整體管理系統的一部份，乃是根據企業風險管理的辦法制定，用來規劃(Plan)、執行(Do)、檢核(Check)、改善(Act)，依序進行 PDCA 模型循環進行風險處理與降低、改善、接受風險。並協助組織建立、實行、運作、監控、審查、維護及改善關於組織整體資訊安全的風險，藉由完整資訊安全控制措施的考量，進一步有效管理資料外洩的風險，針對個人資料之管理系統的 BS 之 PDCA 循環圖如圖 2-7 所示。



Plan	To plan for the implementation of a PIMS	Clause 3
Do	To implement and operate the PIMS	Clause 4
Check	To monitor and review the PIMS	Clause 5
Act	To improve the PIMS	Clause 6

圖 2-7 PDCA 循環圖

資料來源:ISO/IEC JCT 1/SC 27 N9001

PDCA 模型的採用也是反映經濟合作暨發展組織(Organization for Economic Co-operation and Development, OECD)指導綱要。OCED 應用在所有治理資訊系統與網路安全指導綱要中各項原則的政策與運作等級。為適用於 ISMS 過程之 PDCA 管理循環模式：

ISO27001 總共有 11 個領域、39 個控制目標，以及 133 個控

制項目。最主要這些控制目標、控制項目具體表現出資訊安全管理系統(ISMS)的缺失、預防、改善與查核重點。所謂的 11 個領域分別為資訊安全政策(A.5)、資訊安全組織(A.6)、資產管理(A.7)、人力資源管理(A.8)、實體與環境安全(A.9)、通訊與作業管理(A.10)、存取控制(A.11)、資訊系統獲取、開發及維護(A.12)、資訊安全事故管理(A.13)、營運持續管理(A.14)、遵循性(A.15)。

而 39 個控制目標是 11 個領域下再細分，133 個控制項則是 39 個控制目標下再去細分的;若有不足亦可自行擴充如表 2-3 與表 2-4 所示。由此可見，ISO/IEC 27001 對於資訊安全的定義與分類是非常完整與詳細，每一個條款能讓我們更有效率的將違反事件利用到 ISO/IEC 27001 規範標準。資訊安全最終目標是確保資訊的機密性、完整性、可用性三大要素。

這三大要素的說明如下：

-機密性(Confidentiality)：資訊是不可揭露給未經授權個人、個體或組織保護重要資訊不被非法存取或竊取。

-完整性(Integrity)：保護資產精準性與完整性，確保機密資料

未被不當的修改與損害。

-可用性(Availablity)：經過授權使用者因應需求可存取與可使用的資訊。

表 2-2：涉及個人資料之資訊分享宜參考之資訊安全管理系統要求事項

<table>
<tr><td colspan="4">ISO/IEC 27001:2005(E)本文第 4 節~第 8 節之釋義均擴增之</td></tr>
<tr><td colspan="4">5. 安全政策 [1,2,2,0,0]</td></tr>
<tr><td colspan="4">6.組織資訊安全 [2,11,2,0,0]</td></tr>
<tr><td colspan="4">7. 資產管理 [2,5,2,7,0]（備考：新增 1 控制目標）</td></tr>
<tr><td>8. 人力資源安全 [3,9,0,0,1]</td><td>9. 實體與環境安全 [3,13,13,6,3]</td><td>10. 通信與作業管理 [10,32,24,3,11]</td><td rowspan="2">12. 資訊系統獲取、開發及維護 [6,16,3,1,2]</td></tr>
<tr><td colspan="3">11. 存取控制 [7,25,10,2,6]</td></tr>
<tr><td colspan="4">13. 資訊安全事故管理 [2,5,2,1,1]（備考：新增 1 控制目標）</td></tr>
<tr><td colspan="4">14. 營運持續管理 [1,5,2,0,0]</td></tr>
<tr><td colspan="4">15. 遵循性 [3,10,3,0,0]</td></tr>
<tr><td colspan="4">備考：
1.[m,n,o,p,q] - D[控制目標數, 控制措施數, 擴增控制措施數, 新增控制措施數, 強制性控制措施數]
2. 控制目標於 ISO/IEC 3rd WD 27010:2010-05-27 中均擴增之。</td></tr>
</table>

資料來源：ISO/IEC 3rd WD 27010:2010-05-27、ISO/IEC 27011:2008-12-15 與 ISO 27799:2008-07-01。

表 2-3 IS-ISMS 敘述為應(Shall)之強制性控制措施表

ISO/IEC 27002:2005(E)節碼	ISO/IEC 27002:2005(E)之節碼名稱
無	備考：於共享資訊交換作業中確保存在適當之防護
A.8.3.3	存取權限的移除
A.9.2.5	場所外設備的安全
A.9.2.6	設備的安全汰除或再使用
A.9.2.7	財產的攜出
A.10.1.2	變更管理
A.10.1.4	開發、測試及運作設施的分隔
A.10.3.2	系統驗收
A.10.4.1	對抗惡意碼的控制措施
A.10.5.1	資訊備份
A.10.7.2	媒體的汰除
A.10.7.3	資訊處理程序
A.10.8.1	資訊交換政策與程序
A.10.8.2	交換協議
A.10.10.3	日誌資訊的保護
A.10.10.6	鐘訊同步
無	備考：於存取控制之一般性(General)要求(Requirements)。
A.11.1.1	存取控制政策
A.11.2.1	使用者註冊
A.11.2.2	特權管理
A.11.6.1	資訊存取限制
無	備考：於共享資訊主題之唯一識別
A.12.2.4	輸出資料確認
無	備考：建立早期預警系統(Early Warning System)提供資訊安全警示分享資訊

資料來源: 樊國楨、黃健誠，個人資料保護與資訊安全管理之探討，異術科技股份有限公司、國立臺灣大學資訊管理學研究所，2010年9月11日

3.1 個人資料保護與資訊安全治理

個人資料保護法是規範有關個人資料蒐集、處理及利用的行為，為了避免人格權受侵害，並促進個人資料之合理利用，都受到此法的規範。個人資料保護法適用之範圍，涵蓋所有的公務機關及公務機關以外之自然人、法人或團體，衝擊之大，遍及全國所有企業和民眾。個人資料保護法對於必須保護的個人資料類型有明確的界定，包括個人的姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料(Personal Identifiable Information,PII)。(ISO/IEC FCD 29100 4.4 Recognizing PII 如何辨別個人識別資料)

企業在蒐集、處理及利用個資時，必須遵循個資法的規範。企業若發生個資外洩的情事，依個人資料保護法之規定，企業主除須面臨最高 5 年以下有期徒刑，亦可能需賠償最高 2 億元的總額。

有鑒於此法舉證責任課在企業身上，且明列只要企業能證明其無故意或過失者才可免責，但要符合無故意或過失的要件，恐怕相當困難。面對個人資料保護法可能對企業帶來的衝擊，企業

更需對其充分瞭解，並能因應調整企業內部流程及資料的控管機制，國際標準的資訊安全管理系統(ISO/IEC 27001)正符合企業的需求。目前國內已有數百個政府單位、醫院、大學及企業組織建置此資訊安全管理系統並通過認證。

ISO/IEC JTC 1/SC 27 WG5 於 2010 年 6 月 10 日提出隱私參考架構如圖 2-8:

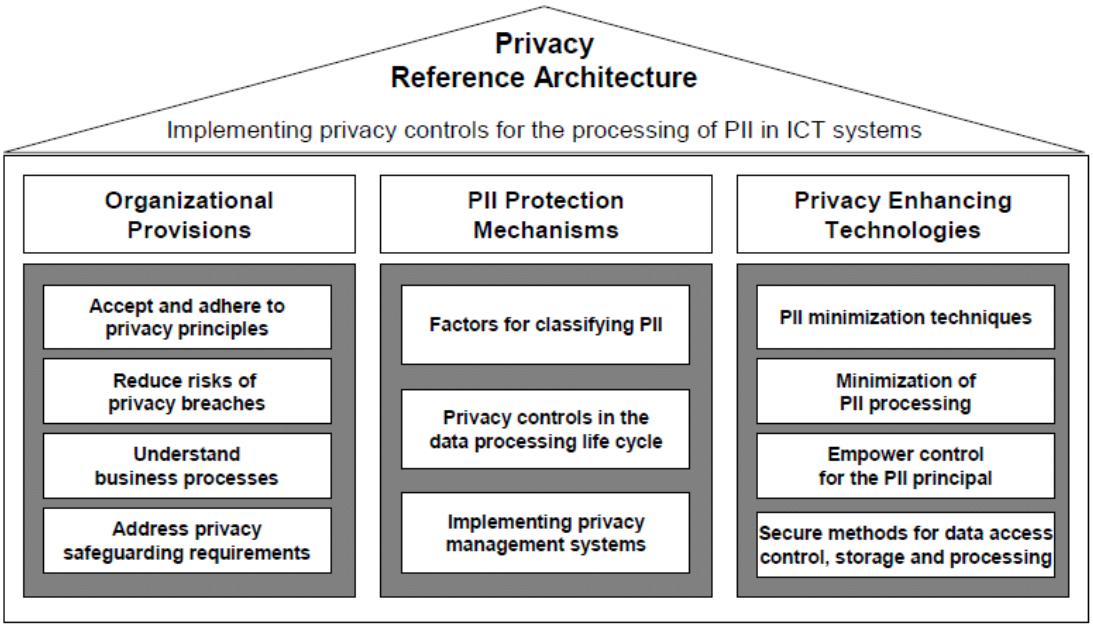


Figure 1 – Main elements of privacy reference architecture

圖 2-8 隱私參考架構的主要元件圖

資料來源: ISO/IEC FCD 29100

其架構共分為三大項:

1. 組織的預防措施
2. 個人資料保護機制

3. 加強隱私技術

於第二節所討論的 ISO/IEC 3rd WD 27014 資訊安全治理框架圖 2-5 裡的資訊及相關技術的控制目標(control objective for information and Related Technology,COBIT)的五大目標做為治理組織於個人資料保護上達到有效性、效率性、保密性、完整性、可用性、遵循性、及可靠性等七大 COBIT 的資訊品質目標，如圖 2-9。

圖 2-9 COBIT IT 治理聚焦區域

資料來源: Control Objectives for Information and Related Technology 4.1，頁 6，圖 2

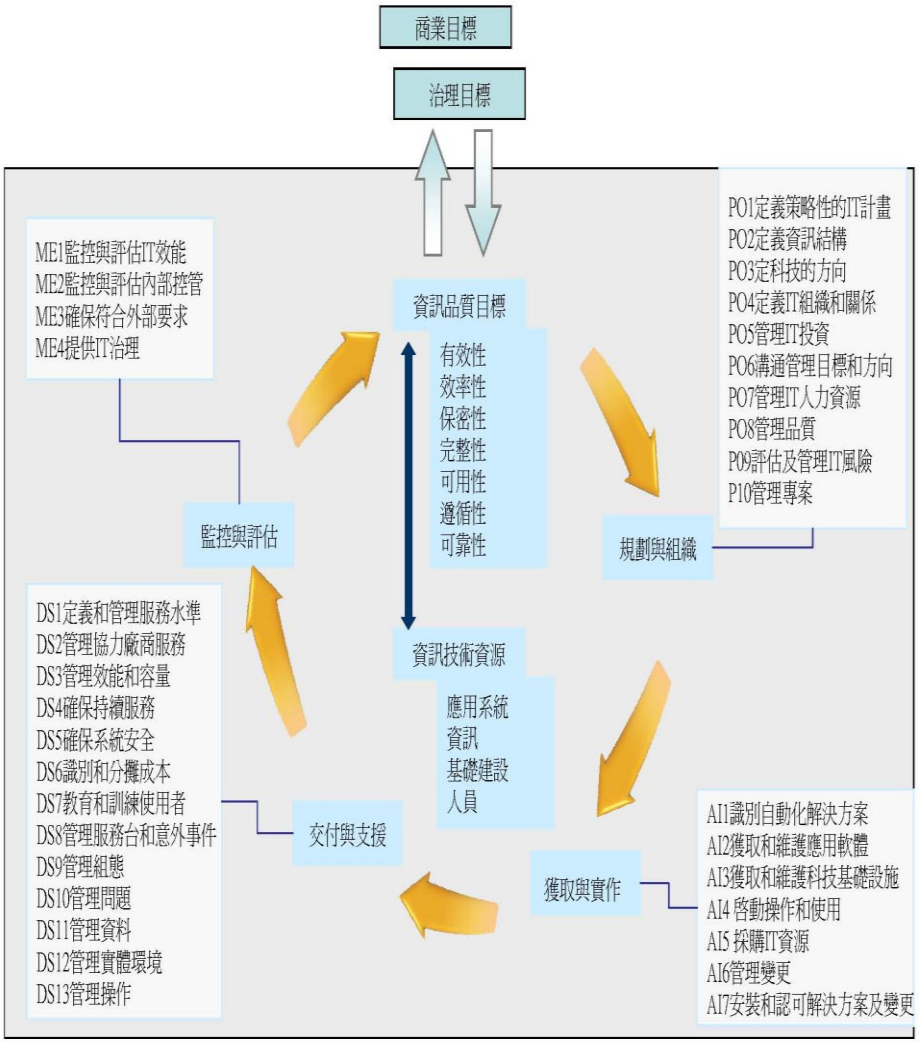


圖 2-10 COBIT 整體架構

資料來源: Control Objectives for Information and Related Technology 4.1，頁 26，圖 23

第一大項「組織的預防措施」裡的接受與堅持組織對保護隱私之原則(Accept and adhere to privacy principle)於 COBIT 整體架構(圖 2-10)內的規劃與組織階段就必須先確認、評估及

管理。

風險程序可減少個人資料外洩之風險(Reduce risk of privacy breaches)，於 P04 定義組織和關係時先了解業務流程(understand business processes)，於 P03 定科技的方向制定個人資料(隱私)的保護要求(Address privacy safeguarding requirement)。因應「個人資料保護法」之立法，公司或組織先接受及堅持組織對保護隱私之原則，再檢查內部業務流程及處理個人資訊流程（如個資種類、數量及是否委外管理等之現況分析)，制定個人資料(隱私)的保護要求。

第二項「個人資料保護機制」中，先將個人資料分類、在研擬出隱私資料的控制生命週期、建置隱私的管理系統，可由 COBIT 提出之獲取與實作對適當的隱私資源及個人資料做出最佳的管理及有效的保護，提供個人資料保護系統機制，儘早對員工進行宣導、講習，資訊安全政策公告於網站中，建議應定期統計點閱率及分析點閱者，以追蹤員工對資訊安全政策了解程度。

等。

第三項「加強隱私技術」均歸類於獲取與實作內，實作後對個人資料保護技術、過程的精減，加強對主要個人資料的控制及

提供更安全的資料存取控制和流程。

但因隱私參考架構沒有提出在資訊安全治理時完整的架構，所以建議加上後續的交付與支援及監控與評估以完整組織資訊安全於個人資料保護的治理架構。

第四節ISO/IEC JTC 1/SC27 對雲端運算之觀點

隨著網路技術及軟硬體的日益發展，雲端運算（Cloud computing）漸漸被業界所採用是不可避免的，是根基於網際網路的運算方式，透過這種方式，共享的軟硬體資源和資訊可以按需要提供給電腦和其他裝置。

台灣經濟部於民國九十九年四月提出「雲端運算產業發展方案」，內容提到「雲端運算是未來十年資訊應用的新主流，各國政府都爭相投入雲端運算政策規劃，值此發展初期，台灣絕不能缺席，更應上緊發條、全力準備出擊。」(經濟部，雲端運算產業發展方案，民國 99 年 4 月，頁 1)。更顯示出台灣政府對雲端運算產業發展的決心及重要性。

雲端運算是繼 1980 年代大型電腦到用戶端-伺服器的大轉

變之後的又一種巨變。使用者不再需要了解「雲端」中基礎設施的細節，不必具有相應的專業知識，也無需直接進行控制。雲端運算描述了一種基於網際網路的新的 IT 服務增加、使用和交付模式，通常涉及透過網際網路來提供動態易擴充功能而且經常是虛擬化的資源。雲端其實是網路、網際網路的一種比喻說法。因為過去在圖中往往用雲端來表示電信網，後來也用來表示網際網路和底層基礎設施的抽象。典型的雲端運算提供商往往提供通用的網路業務應用，可以透過瀏覽器等軟體或者其他 Web 服務來存取，而軟體和資料都儲存在伺服器上。雲端運算關鍵的要素，還包括個性化的使用者體驗。

雲端運算可以認為包括以下幾個層次的服務：

雲端軟體 Software as a Service (SaaS):

打破以往大廠壟斷的局面，所有人都可以在上面自由揮灑創意，提供各式各樣的軟體服務。 參與者：世界各地的軟體開發者。

雲端平台 Platform as a Service (PaaS):

打造程式開發平台與作業系統平台，讓開發人員可以透過網路撰寫程式與服務，一般消費者也可以在上面執行程式。 參與者：

Google、微軟、蘋果、Yahoo!。

雲端設備 Infrastructure as a Service (IaaS):

將基礎設備（如 IT 系統、資料庫等）整合起來，像旅館一樣，分隔成不同的房間供企業租用。 參與者：英業達， IBM、戴爾、昇陽、惠普、亞馬遜。

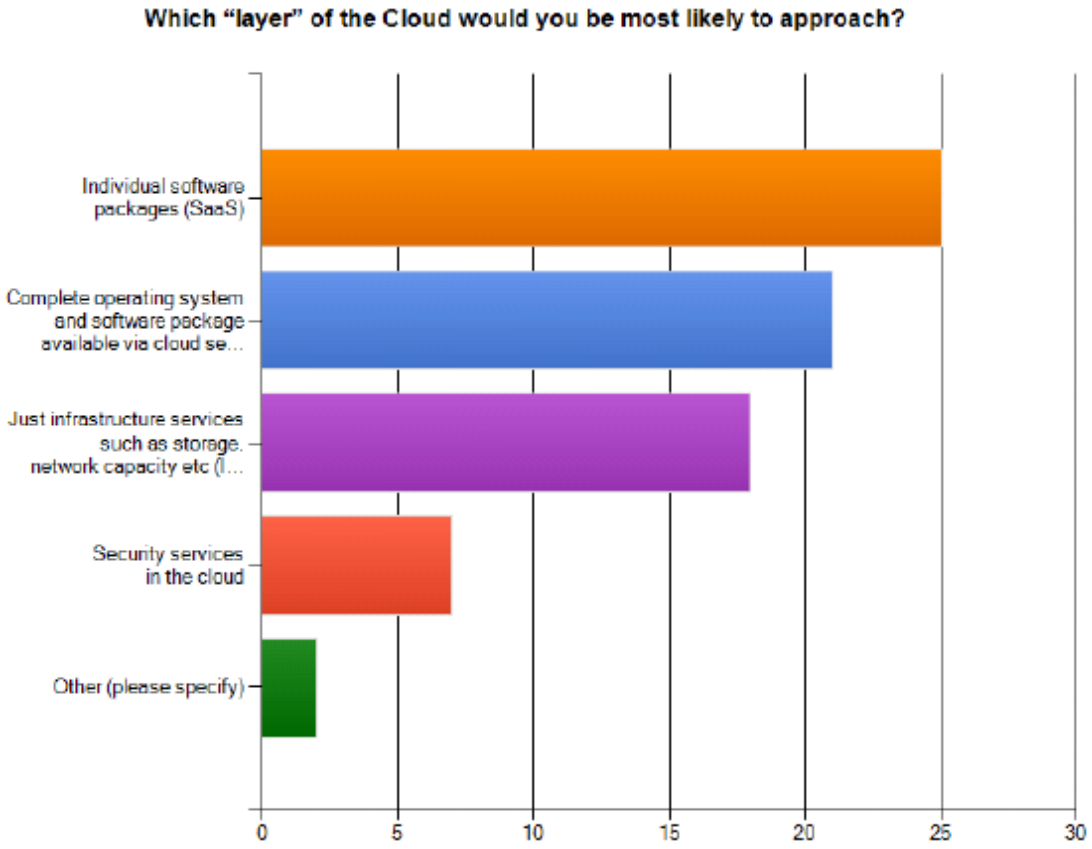


圖 2-11 中小型企業對雲端服務之選擇

來源: ISO/IEC JTC 1/SC27 N9314 : A SME perspective on cloud computing – Survey PG. 10

歐洲網路與資訊安全機構(European Network and

Information Security Agenc,ENISA)對於中小型企業調查，顯示目前中小型企業利用雲端服務比較偏好使用雲端軟體多於雲端平台及設備如圖2-11，這裡隱藏了關於隱私及資訊安全之相關議題，例:機密文件的安全性，CP (Cloud Provider)基礎設施的可靠性。

雲端之模型:

公有雲(public cloud):由無任何關係之公司管理及擁有。

私有雲(Private cloud):公司內部自行管理及擁有。

夥伴雲(Partner cloud):與企業夥伴共同管理及擁有。

聯邦雲(Federation cloud): 美國聯邦政府使用。

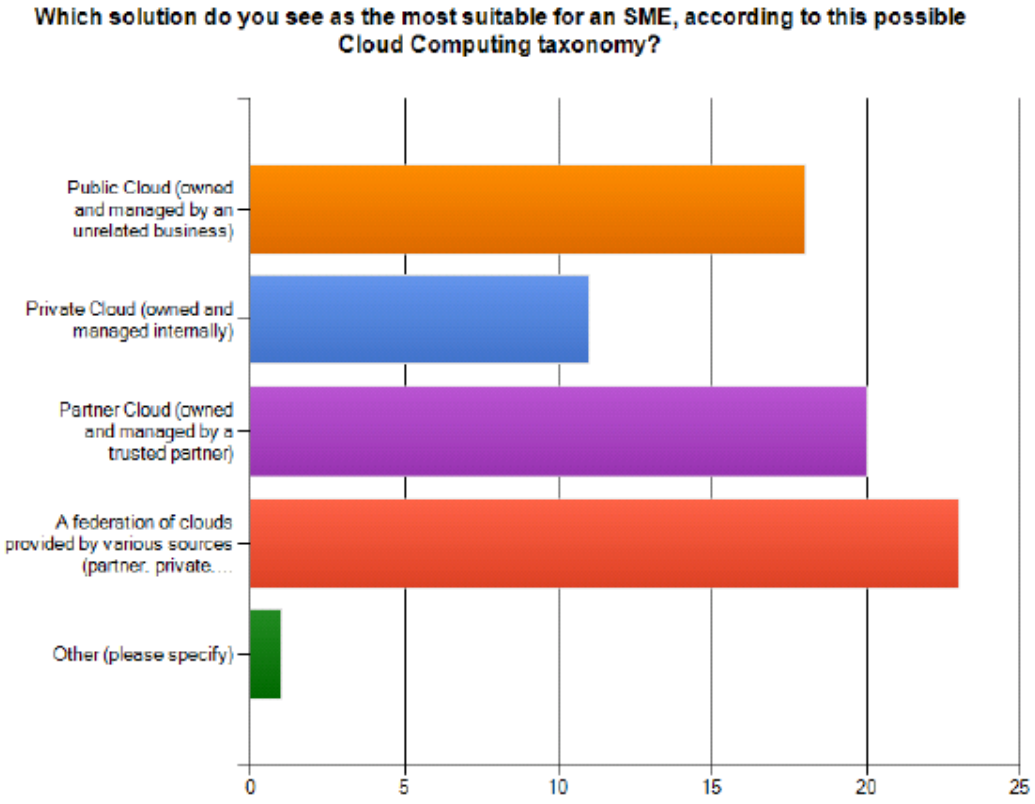


圖 2-12 中小型企業對雲端模型之選擇

來源: ISO/IEC JTC 1/SC27 N9314 : A SME perspective on cloud computing –Survey 第 9 頁

ENISA(European Network and Information Security Agency)對中小型企業做調查，顯示目前中小型企業利用雲端技術比較偏好於和其他的公司或機構一起使用，於自行管理及擁有者比重較為少如圖 2-12，原因在於經濟規模(Economic Scale)較小，而私有雲對中小型企業會是較重的負擔。

雖然雲端對未來的資訊發展看起來很方便、省資源、省空間，但是對於隱私及安全議題來說，就沒有這麼的輕鬆，圖 2-13

表示中小型企業對於雲端運算最關注之安全議題，有隱私、企業機密資料、服務或資料的有效性、服務或資料的整合性、喪失服務或資料控制力，由於雲端服務是透過網路來進行大量存取，所以在個人資料保護及資訊安全管理上漸漸的萌發出了一些問題。

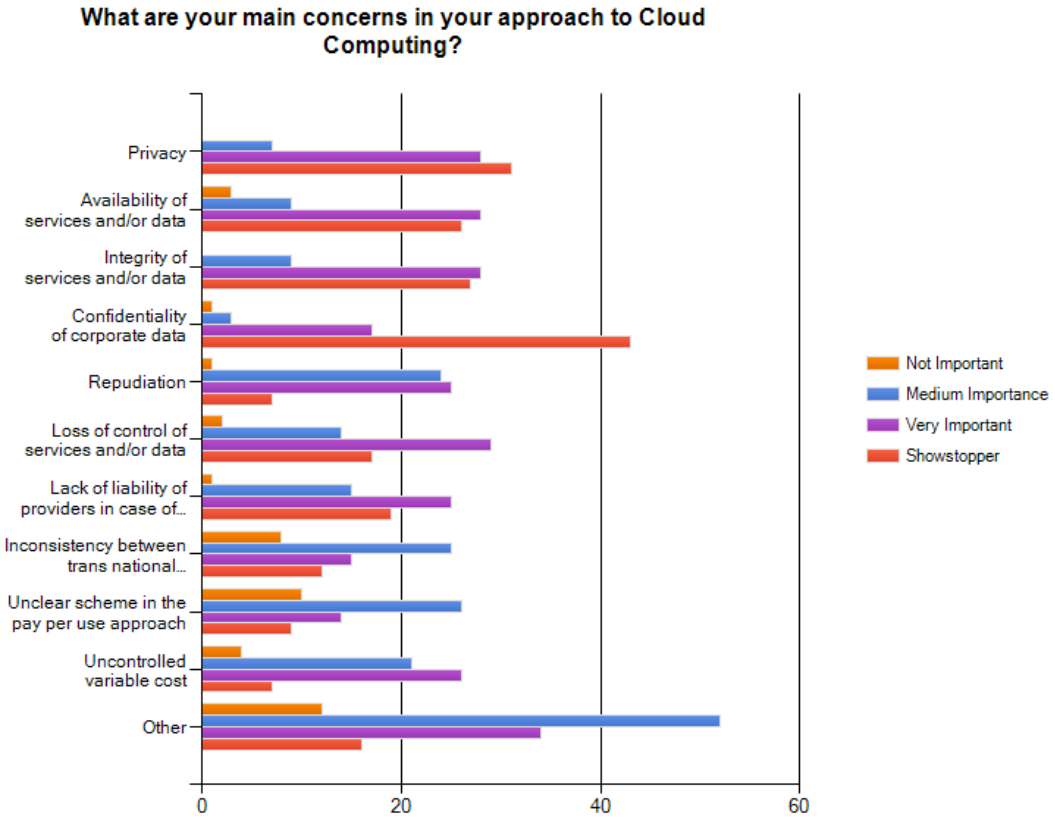


圖 2-13：中小型企業對雲端技術最關注的安全議題

來源: ISO/IEC JTC 1/SC27 N9314 : A SME perspective on cloud computing – Survey 第 16 頁

ISO/IEC JTC 1/ SC27 WG 5 於 2010-09 發了兩份文件

(ISO/IEC JTC1/SC 27 N9326 雲端架構及 ISO/IEC JTC1/SC 27 N9314 資訊安全議題)給其會員，要求於 2010-09-30 紐約的會議中討論對於雲端運算之相關議題。

目前對雲端運算(Cloud Computing)這個產業來說，並沒有一個明確的規範或是慣用的合約，所以對各個中小型企業在簽約時必須和自己的雲端提供商做談判爭取對己方最有利的合約，表 2-4 顯示談判的三種模式。

表 2-4 大型企業和中小型企業於雲端合約談判的三種模式

CLOUD PROVIDER	CUSTOMER
A) Large company – **strong ability to negotiate contract clauses**	SME – **Weak or lacking ability to negotiate contract clauses**
B) Both the customer and the provider have the **ability to negotiate contract clauses**	
C) SME – **Weak ability to negotiate contract clauses**	Large company or public administration - **may negotiate contract clauses**

Depending on the particular case (whether it is A, B or C), the way to tackle the issues identified in *subsection* I may differ significantly.

資料來源: ENISA, Cloud computing-Benefits, risks and recommendations for information security, pg. 98

為因應不同的行業(如:電信業，支付卡行業)，其各有不同的資訊安全規範(如:ISO/IEC 27011，PCI DSS)，所以在和雲端供應商(Cloud Provider)簽合約時特別需要注意行業內之資訊

安全規範，核簽訂有效的服務水準協議(SLAs,Service level agreements)，以免造成後續無法申請證照或稽核失敗之困擾。雲端運算對於資訊安全的益處有下列幾點:

1. 市場規模的安全與效益(Security and the benefits of scale)
2. 市場差異帶來的安全效益(Security as a market differentiator)
3. 標準化管理介面的安全服務(Standardised interfaces for managed security services)
4. 用於快速，智慧配置(Rapid, smart scaling of resources)
5. 審核和證據收集(Audit and evidence-gathering)
6. 更及時，有效和高效的更新和還原(More timely and effective and efficient updates and defaults)
7. 審核和服務合約驅使更好的風險管理(Audit and SLAs force better risk management)
8. 資源集中的優勢(Benefits of resource concentration)

雲端運算對於資訊安全的風險有下列幾點:

1. 政策及組織的風險(Policy and organizational risks)

2. 技術風險(Technical risks)

3. 法律風險(Legal risks)

目前 WG5 還繼續在研究雲端運算的資訊安全相關議題，現階段採根基於 ISO/IEC 27001/2 、BS 25999 及 NIST Special Publication 800-53 (修定第三版)，對雲端運算的資訊安全管理提出建議，在目前還沒有明確的規範時，要求每年的 ISMS 報告書能遵守 ISO/IEC 27001 的基本規範以達到符合基本安全之標準。

第三章　案例探討

第一節 Sony Play Station Network 遭駭之案例

3.1.1 案例介紹

(關於 Sony 遭駭之相關文章於附件一、附件二)

日本時間 2011 年 4 月 20 日，Sony 首次偵測到非授權的存取，在初步判斷對方是高手中的高手後，就立刻延請第二家資料安全公司進駐，來分析該入侵者以及其造成的影響，隨後就寄出信件來警告使用者；事後則發現有很多資料被竊取，不過關於信用卡的資訊(卡號、到期日、帳單地址等)，Sony 表示沒有證據顯示這些資料也被偷走，不過 Sony 方面目前也沒有確認是否有任何跟信用卡有關的詐欺事件發生，有任何消息會公告周知，據信他們可能也不很清楚。

平井一夫表示，Sony 已經在著手部屬新的安全措施，以避免未來發生類似的事件;將會在美國聖地牙哥的新資料中心安插更先進的安全性防護，從加強的外部侵入感應、自動軟體偵測、資料加密層級提高等等相關的改善，另外也會多蓋幾道防火牆；另外 Sony 也提醒使用者，近期要仔細核對信用卡的相關資訊

（包括帳單），並且更改所有的密碼，以及任何跟 PSN 帳號密碼相同的其他網路服務帳號密碼。Sony 還說他們會考慮替受影響的 PSN 用戶支付新 PSN 信用卡發行所需的費用，同時已經確定會提供 30 天的免費 PS Plus 會員服務、30 天的免費 Music Unlimited 服務（Qriocity），外加一些特定遊戲、軟體內容的免費下載；而整個 PSN 服務的恢復，預計會在一個月內完成。

3.1.2 案例分析

這個事件告訴我們像 PS3 這種半封閉系統並不會比較安全，而且製造商容易在安全性上鬆懈，主要的理由為:

1.PS3 並不像 PC 一樣普遍，因此製造商會覺得不易成為駭客目標

2.系統為半封閉式（embedded），用戶無法隨意安裝軟體，製造商會覺得要破解與 Server 端的封包有難度

3.連回 PSN 會用 Hardware ID 辨識去限定 PS3 only，一般 PC 無法直接連到 PSN，製造商會認為這樣就已經降低不少風險。

但去年底卻發生了第一個警訊，PS3 韌體招破解，可以用 jailbreak 方式可以玩硬碟上非授權的遊戲軟體既然韌體遭破

解，想要抓取與 PSN 間的傳輸資料也不難了。

依 Sony 5/1 日的說明(附件二)，推斷 PSN 只有佈建一層防火牆，且沒有 IPS/IDS 系統監控，駭客應該透過入侵 web server 取得資料庫帳號，再直接進入資料庫將資料全部傳走，Sony 應該是發現大筆資料被複製走才發現事情大條，進而馬上關閉 PSN 服務。

以下是駭客的攻擊方式：

1. 資料庫隱碼攻擊

模擬封包對 PSN server 進行隱碼攻擊，取得用戶相關 table 欄位資料。一般初級工程失常犯的錯，由於一般市售教學書籍範例大都是錯的，照著範例兜出 SQL 語法容易鑄成大錯

2.Web server 安全漏洞

利用 PSN web server 漏洞，入侵 web server，再利用 web server 帳號登入 Database 將 DB 全都 Dump 走。 這類問題通常發生在系統未定時做安全性更新且沒有 IDS 系統監控入侵指令，web server 在公開的環境是最容易被攻擊的，一旦被取得 web server 的 account，很容易變成跳板入侵資料庫。

3. 用戶密碼、信用卡等重要資料無嚴謹的加密

依 Sony 公佈的資料，他們信用卡資料有加密，但卻沒有公佈用哪一種加密方式，目前常見的有 MD5、DES、RSA，其中 DES 及 MD5 都有破解工具，RSA 雖然比較嚴謹，但還是有被破解的可能，Sony 說用戶密碼是用雜湊的方式保護，應該是用 MD5 方式儲存，因此建議用戶在重新登入 PSN 時更改密碼。其實加密資料對於執行效率一定有影響，但卻可以在資料被盜取後最最後一關的保護。

3.1.3 由雲端運算服務看 Sony 事件

由 ISO/IEC JTC 1/SC 27 N9314 ENISA, Cloud Coputing-Benefits Risk,and Recommandation for information security 裡提到的多項風險來看這次 Sony 的事件。

下列表所示之 R#=風險(Risks)，V#=弱點(Vulnerabilities)，A#=資產(Assets)是於 N9314 文件內圖表所分析之代號:

R.5 雲端服務終止或失敗:

表 3-1 雲端服務終止或失敗之風險

Probability	N/A	
Impact	VERY HIGH	Comparative: Higher
Vulnerabilities	V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A9. Service delivery – real time services A10. Service delivery	
Risk	**MEDIUM**	

資料來源: ISO/IEC JTC 1/SC 27 N9314 ENISA, Cloud Coputing- Benefits Risk,and Recommandation for information security,pg 31

當 Sony PSN 服務暫停時，而導致 Sony 的公司聲譽受到影響、顧客的信任下降、服務無法傳遞等公司資產受到影響如表 3-1。

R.12 數據攔截:

表 3-2 數據攔截之風險

Probability	MEDIUM	Comparative: Higher (for a given piece of data)
Impact	HIGH	Comparative: Same
Vulnerabilities	V1. AAA vulnerabilities V8. Communication encryption vulnerabilities V9. Lack of or weak encryption of archives and data in transit V17. Possibility that internal (cloud) network probing will occur V18. Possibility that co-residence checks will be performed V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A2. Customer trust A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A23. Backup or archive data	
Risk	**MEDIUM**	

資料來源: ISO/IEC JTC 1/SC 27 N9314 ENISA, Cloud Coputing- Benefits Risk,and Recommandation for information security,pg 38

於 2011 年 4 月 20 日 Sony 的數據遭攔截，其直接或間接地影響到了公司聲譽、顧客的信任度、智慧財產、個人敏感性資料等，如表 3-2。

R.17 丟失加密金鑰

表 3-3 丟失加密金鑰之風險

Probability	LOW	Comparative: N/A
Impact	HIGH	Comparative: Higher
Vulnerabilities	V11. Poor key management procedures V12. Key generation: low entropy for random number generation	
Affected assets	A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A12. Credentials	
Risk	**MEDIUM**	

資料來源: ISO/IEC JTC 1/SC 27 N9314 ENISA, Cloud Coputing- Benefits Risk,and Recommandation for information security,pg 41

Sony 表示用戶密碼是用碎映的方式保護，其使用 MD5 方式來儲存，因此建議用戶在重新登入 PSN 時更改密碼。由此可見其做法對加密的方法及保護都是不夠的，可能影響到的公司資產有智慧財產、個人敏感性資料、HR 的資料如表 3-3。

第二節北京市人民法院審理王菲個人資料侵權案例

3.2.1 案例介紹

(完整判決書於附件三)

北京市民王菲與死者姜岩係夫妻關係，雙方於 2006 年 2 月

22 日登記結婚。2007 年 12 月 29 日，姜岩從自己居所的 24 層樓高處跳樓自殺。

姜岩生前在網路上註冊了博客，並進行寫作。在自殺前 2 個月，姜岩關閉了自己的博客，但一直沒有中斷博客的寫作。姜岩在博客中以日記形式記載了自殺前兩個月的 心路歷程，將王菲與案外女性東某的合影照片貼在博客中，認為二人有不正當兩性關係，自己的婚姻很失敗。姜岩的日記顯示出了丈夫王菲的姓名、工作單位位址等 資訊。姜岩在第一次自殺（2007 年 12 月 27 日）前將自己博客的密碼告訴一名網友，並委託該網友在 12 小時後打開博客。在姜岩第二次自殺（2007 年 12 月 29 日）死亡後，姜岩的網友將博客密碼告訴了姜岩的姐姐姜紅，姜紅將姜岩的博客打開。

姜岩的博客日記被一名網友閱讀後轉發在天涯網中，後又不斷被不同網友轉發至其他網站上，姜岩的 死亡原因、王菲的“婚外情”等情節引起越來越多網友的長時間持續關注和評論。許多網友認為王菲的“婚外情”是促使姜岩自殺的原因之一；一些網友在進行評論 的同時，在天涯論壇、大旗網等網站上發起對王菲的“人肉搜索”，使王菲的姓名、工作單位、家庭

住址等詳細個人資訊逐漸被披露；一些網友在網路上對王菲進行謾罵；更有部分網友到王菲及其父母住處進行騷擾，在王家門口牆壁上刷寫、張貼“無良王家”、“逼死賢妻”、“血債血償”等標語。直至本案審理期間，許多互聯網網站上仍有大量網友關於此事的評論文章。

3.2.2 案例分析

天涯網於自行的網頁內就設有對敏感性資料的控制措施，而其之後也立即對網友發表的帖子及個人資料資訊加以進行刪除，對此北京人民法院判決王菲對天涯網告訴一案全部訴訟請求遭到駁回。對此證明了個人保護法是不可以無限上網。

雖然如此本案例內關於網友發動人肉搜索來獲得王菲之個人資料將之公開所照成的侵害，目前於台灣目前個人資料保護法沒有針對人肉搜索此項舉動作明確的規範，本論文以中國的案例來做討論。

而於資訊隱私權侵害的類型定義區分為下列兩大項:

1. 個人資料隱私權之侵害

(1) 使用者自行提供之資料遭侵害。

(2) 第三人提供知他人個人資料。

(3) 利用科技手段獲得之個人資料

2. 通訊隱私權之侵害:如對公司員工之電子郵件監控

網友之人肉搜索之個人資料侵害型態包含了

1. 搜索引擎利用

2. 公佈各人困窘之私事(文字、圖片、影音媒體檔)

3. 侵入私人財產、干擾私人生活安寧

基於上述之侵害型態，ISO/IEC 27001 中的控制措施如下:

(A.10.2.2)第三方服務的監視及審查

(A.11.1.1)存取控制政策

(A.11.6.1)資訊存取限制

第四章　支付卡行業資料安全標準對雲端運算之應用

「資訊產業應朝高附加價值的軟體及服務發展;政府與企業則須從應用雲端運算，提升經營效率。」(經濟部，雲端運算產業發展方案，民國 99 年 4 月，頁 1)，欲發展雲端運算行業，必然須先了解其相關的主要問題，ISO/IEC JTC 1/SC 27 N9314 ENISA, Cloud Coputing- Benefits Risk,and Recommandation for information security,Pg.97, 附件 1，提到凡討論雲端運算任何案例必須有下列五大項的主要法律問題:

1 資料保護

A. 可用性和完整性

B. 最低標準或保證

2. 機密性

3. 智慧產權

4. 專業疏忽

5. 外包服務和控制變化

根據此五大項提出建議遵照的國際標準規範來制定合乎雲端運算之規範，因為目前國際標準規範內於雲端運算還沒有明確

的規範章程，主要是依據 ISO/IEC 27001 來做相關的參考準則，而外包廠商的法律問題對於雲端運算是首當其衝最為重要的議題之一，本論文將探討 ISO/IEC 27001 之不足，以支付卡行業(PCI) 資料安全標準 (DSS)的相關文件應用於雲端運算之外包服務主要規範，使得中小型企業在使用雲端運算服務時簽訂服務水準協議(SLAs)對而外包廠商有一個規範的依據。

4.1 支付卡行業 (PCI) 資料安全標準 (DSS)介紹

支付卡行業 (PCI) 資料安全標準 (DSS) 促進並提高持卡人資料安全，有利於全球廣泛採用統一的資料安全標準。其提供用於保護持卡人資料安全的技術與作業要求之基準，適用於所有涉及支付卡處理之實體，包括商戶、處理機構、購買者、發行商和服務提供商以及儲存、處理或傳輸持卡人資料的所有其他實體，所以其運作模式與雲端運算有其相同之處。PCI DSS 包括保護持卡人資料的基本要求，其規範已有對個人資料作基本的保護規範，並可以增加額外的管控措施對 ISMS 實際環境上作修改及調整，以進一步降低風險，表 4-1 是 PCI DSS 要求的高級概要介紹。

表 4-1 PCI 資料安全標準

PCI 資料安全標準 - 高級概觀

建立並維護安全網路	1. 安裝與維護防火牆設定以保護持卡人資料 2. 對於系統密碼及其他安全參數，請勿使用供應商提供的預設值
保護持卡人資料	3. 保護儲存的持卡人資料 4. 加密透過開放的公用網路傳輸的持卡人資料
維護漏洞管理程式	5. 使用並定期更新防毒軟體或程式 6. 開發並維護安全系統和應用程式
實施嚴格的存取控制措施	7. 限制為只有業務需要知道的人才能存取持卡人資料 8. 為具有電腦存取權的每個人指定唯一的 ID 9. 限制對持卡人資料的實際存取
定期監控並測試網路	10. 追蹤並監控對網路資源及持卡人資料的所有存取 11. 定期測試安全系統和程序。
維護資訊安全政策	12. 維護滿足所有人員資訊安全需求的政策。

資料來源:支付卡行業資料安全標準:要求和安全評估程序(2.0),Pg.5

PCI DSS 安全要求適用於所有系統元件，其定義「系統元件」為包含於持卡人資料環境或與之相關的任何網路元件、伺服器或應用程式。「系統元件」還包括所有虛擬元件，例如虛擬機、虛擬交換機/路由器、虛擬裝置、虛擬應用程式/桌面和 Hypervisor，持卡人資料環境由人員、程序以及儲存、處理或傳輸持卡人資料或敏感驗證資料的技術構成，網路元件包括但不局限於防火牆、交換機、路由器、無線存取點、網路裝置和其他安全裝置。伺服器類型包括但不限於以下類型：Web、應用程式、資料庫、認證、郵件、代理、網路時間協定（NTP）和網域名稱

伺服器（DNS)，應用程式包括所有購買和自訂的應用程式，包括內部和外部（例如網際網路）應用程式，所以其範圍是相當的完整和嚴謹。

PCI DSS 評估的第一步是精確確定審查的範疇。接受評估的實體必須確定持卡人資料的所有位置與流量並確保其包含在範疇之內，以確認範疇的精確度，此事每年至少要做一次且須在年度評估之前完成。

表 4-2 PCI DSS 相關文件

文件	適用對象
PCI 資料安全標準要求和安全評估程序	所有商戶和服務提供商
導覽 PCI DSS：理解資料安全要求的目的	所有商戶和服務提供商
PCI 資料安全標準：自我評估問卷說明和指南	所有商戶和服務提供商
PCI 資料安全標準：自我評估問卷 A 和證明	符合資格的商戶[9]
PCI 資料安全標準：自我評估問卷 B 和證明	符合資格的商戶[9]
PCI 資料安全標準：自我評估問卷 C-VT 和證明	符合資格的商戶[9]
PCI 資料安全標準：自我評估問卷 C 和證明	符合資格的商戶[9]
PCI 資料安全標準：自我評估問卷 D 和證明	符合資格的商戶和服務提供商[9]
《PCI DSS 與 PA-DSS 術語、縮寫和首字縮寫》	所有商戶和服務提供商

資料來源:支付卡行業(PCI)資料安全標準-導覽 PCI DSS-理解資料安全要求之目的，49 頁

4.2 第三方服務提供商及外包之要求

公司可能會使用第三方服務提供商，代替它們儲存、處理或

傳輸持卡人資料，或者管理諸如路由器、防火牆、資料庫、實體安全和/或伺服器等元件，相同的對雲端運算來說個人、公司或政府也會使用第三方服務提供商相同的服務，尤其談到第三方服務提供商處理敏感型資料，例如個人資料時，對個人資料安全產生的影響，且在資訊安全治理時於「交付及支援」需要考量的重要一環(如圖 2-10，頁 39)。

組織或公司對於資料的儲存、處理或傳輸此等服務外包給第三方服務提供商的實體，必須詳細記錄每家第三方服務提供商的職責，明確的評估實體適用哪些要求，以及公司或組織適用哪些要求，對於公司或組織，有兩個選項可驗證其是否合乎規定：

(1) 可由第三方服務提供商自己執行評估並向公司或組織提供證明其合規性的證據。

(2) 如第三方服務提供商沒有執行評估，公司或組織則需在每次執行評估期間審查自己的服務。

下表為 ISO/IEC 27001 對第三方服務提供商的相關控制措施及使用 PCI DSS 對其做出補充一覽表:

表 4-3 對 ISO/IEC 27001 協力廠商控制措施補充表

ISO/IEC 27001 對協力廠商之相關控制	利用 PCI DSS 之控制措施加以補充

措施	
A.5.1.1 資訊安全性原則文件 控制措施 資訊安全性原則文件應經過管理層批准,向所有員工和相關外部團體發佈和溝通；	
A.6.2.3 在協力廠商協議中強調安全控制措施 在與協力廠商合約中應包含所有的安全要求，如訪問、處理、溝通、管理組織的資訊或資訊處理設施,或增加資訊處理設施的產品和服務；	12.8.2 要求協力廠商出具書面合約，由其確認對自己擁有的資料的安全性負責，並保留此合約。
A.10.2 協力廠商服務交付管理 控制目標:實施和維護資訊安全的適當水準,確保協力廠商交付的服務符合協定要求；	12.8.3 確保已建立雇用協力廠商的程序
A.10.2.1 服務交付 控制措施 應確保包含在協力廠商服務交付協定中的安全控制、服務定義、交付級別應由協力廠商去實施、運營和維護；	12.8.1 協力廠商之維護服務提供商清單 12.8.4 維護計劃，以每年至少監控一次協力廠商的遵從性狀態。
A.10.2.2 協力廠商服務的監督和評審控制措施 由協力廠商提供的服務、報告和記錄應定期監控和評審，應有規律的進行審核；	12.8.1 協力廠商之維護服務提供商清單 12.8.4 維護計劃，以每年至少監控一次協力廠商的遵從性狀態。
A.10.2.3 協力廠商服務的變更管理 控制措施 服務提供的改變，包括維護、改進存在的資訊安全性原則、程式和控制措施應被管理,考慮業務系統和過程的關鍵性並再次評估風險；	12.8.1 協力廠商之維護服務提供商清單 12.8.4 維護計劃，以每年至少監控一次協力廠商的遵從性狀態。

A.10.6.2 網路服務安全 控制措施 應識別所有網路服務的安全特性、服務級別和管理要求,並包括在網路服務協定中,無論網路服務是內部提供還是外包;	
A.10.8 資訊交換 控制目標:在保持組織間或組織和外部組織之間交換時資訊和軟體的安全;	2.4 協力廠商必須保護各實體的託管環境與資料。
A.10.8.2 切換式通訊協定 控制措施 應建立組織和外部組織之間的資訊和軟體交換的協定;	
A.12.5.5 軟體外包開發 控制措施 組織應監督和控制軟體外包開發;	
A.13.1.2 報告資訊安全弱點 控制措施 應要求使用資訊系統和服務的所有員工、合同人員及協力廠商人員記錄和報告在系統和服務中觀察或可疑的弱點;	附錄 A.1.4 啟用在任何協力廠商出現漏洞時及時提供取證調查的程序。

資料來源: ISO 27001 資訊技術-安全技術-資訊安全管理系統-要求事項「Information Security Management System (ISMS) - Requirement」和 PCI DSS 要求和安全評估程序 2.0 版,2010 年 10 月及本研究

第五章　結論及建議

第一節　結論

本論文根據 ISO/IEC JTC 1/SC27 WG1 和 WG5 所提出之文件，來探討資訊安全治理、個人資料保護及雲端運算上提出以下綜合建議:

因應「個人資料保護法」之立法，公司或組織先接受及堅持組織對保護隱私之原則，於規劃與組織階段就必須先確認，有效的評估及管理風險程序可減少個人資料外洩之風險，在定義組織和關係時先了解業務流程，制定個人資料(隱私)的保護要求。再檢查內部業務流程及處理個人資訊流程（如個資種類、數量及是否委外管理等之現況分析），制定個人資料(隱私)的保護要求。

先將個人資料分類、在研擬出隱私資料的控制生命週期、建置隱私的管理系統，可由 COBIT 提出之獲取與實作對適當的隱私資源及個人資料做出最佳的管理及有效的保護，提供個人資料保護系統機制，儘早對員工進行宣導、講習，資訊安全政策公告於網站中，建議應定期統計點閱率及分析點閱者，以追蹤員工對資訊安全政策了解程度。

「加強隱私技術」歸類於獲取與實作內，實作後對個人資料保護技術、過程的精減，加強對主要個人資料的控制於資訊安全政策及資訊安全管理系統（ISMS）相關各階文件，應建立定期或於發生資訊安全事件後適時審查及修訂之機制，以保持其有效性及適切性，以提供更安全的個人資料存取控制和流程。

公司或組織使用雲端運算廠商之服務，建議於合約中訂定必要之資訊安全要求(如應交付文件、服務水準協議、智慧財產權、資訊安全規範遵循及稽核權等資訊安全條款)。簽訂合約時特別需要注意行業內之資訊安全規範，核簽訂有效的服務水準協議(SLAs,Service level agreements)，以免造成後續無法申請證照或稽核失敗之困擾。

資訊安全事件通報及處理程序，建議將委外廠商及第三方使用者納入，定期測試演練，並對事件紀錄進行統計及根因分析，且對矯正及預防措施追蹤其改善情形，以落實管理。

第二節　建議後續研究

由於雲端運算必須利用網路來存取資料，再傳送過程期間必須注意到對個人資料的保護，和有效率的存取。由於 Sony 被駭

客攻擊之案例，其組織未對傳送中的資料進行嚴密的保護，其使用的加密技術及程度都是不夠的，導致重要的個人機密及信用卡資訊外洩，建議後續研究雲端系統的實際獲取控制架構，可根基於 ISO/IEC JTC 1/SC 27 N9326 提出圖 5-1 之雲端獲取(ACCESS)資訊的架構:

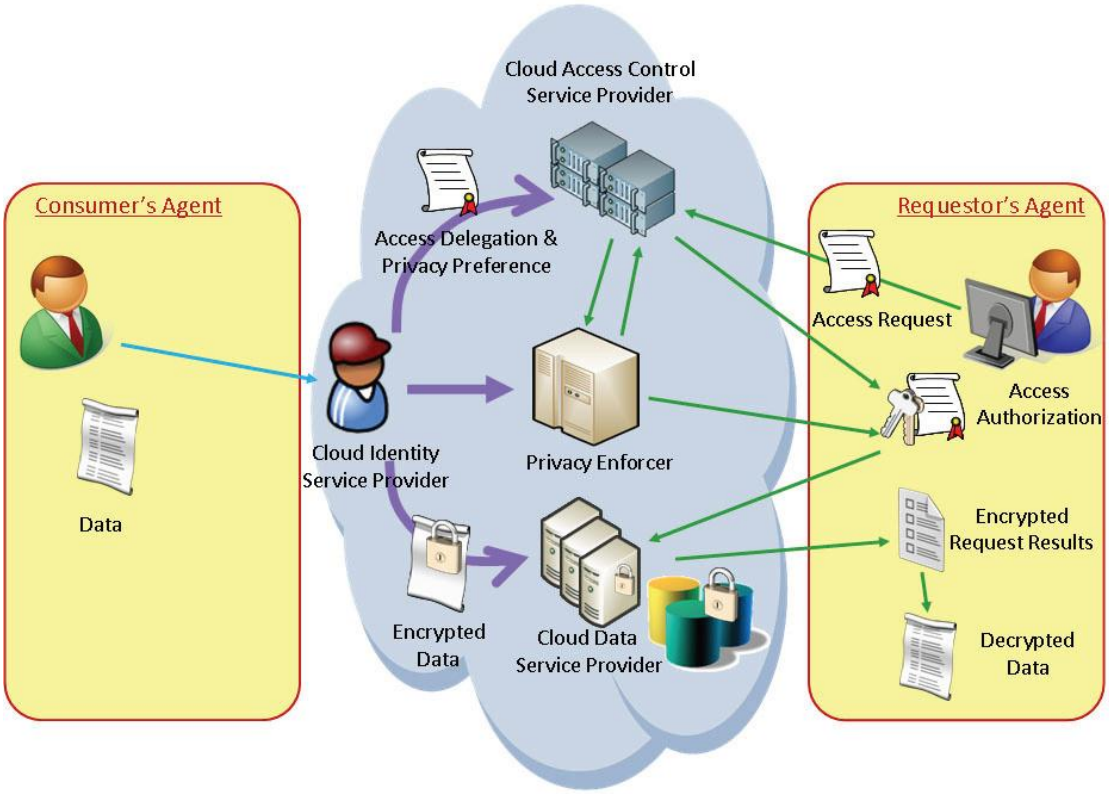


圖 5-1 Better Cloud Computing Architecture for Privacy-Preserving and Usable Data Outsourcing

資料來源：ISO/IEC JTC1/SC 27 N9326 ,Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach,Pg. 11,(May, 2010)

參考文獻

ISO 27001 Certificate website 來源:http://www.iso27001certificates.com/Register%20Search.htm(2011/5/20)。

個人資料保護法 (2010)。

支付卡行業 (PCI)資料安全標準(2010)導覽 PCI DSS-理解資料安全要求之目的2.0 版。

中國人民共和國國家標準(2011)信息安全技術-各人信息保護指南草案。

陳彥如(2010)資訊安全治理之價值交付的研究。

段逸如、方品羚、魏晉暘(2009)網路隱私權保護之研究。

樊國楨、黃健誠、廖菊芳(2011)個人資料保護與資訊安全管理微探, 政府機關資訊安全通報，第 279 期，頁 5-240。

樊國楨、黃健誠、廖菊芳(2011)管理系統標準化簡述-根基於資訊安全管理系統, 政府機關資訊安全通報,第 282 期,頁 4-14。

樊國楨、黃健誠、林樹國(2010)資訊安全管理系統政策微探-根基-政府機關之異地備援個案,前瞻科技與管哩，創刊號(已接受)。

ISO (2005)ISO/IEC 27001Information technology-Security techniques - Information security management systems - Requirements。

ISO (2010)Text for ISO/IEC 3rd WD 27014—Information technology—Security techniques- Information security governance framework。

ISO (2010) ISO/IEC JTC1/SC 27 N8808 Information technology - Security techniques-Privacy reference architecture。

ISO (2010) ISO/IEC JTC1/SC 27 N9226 Information technology - Security techniques-Privacy framework。

ISO (2010) ISO/IEC JTC1/SC 27 4th WD N9001 Information technology - Security techniques - Information security management systems - Requirements。

ISO (2010) ISO/IEC JTC1/SC 27 N9326 Modelling cloud computing architecture without compromising privacy。Pg. 10-11

ISO (2010) ISO/IEC JTC1/SC 27 N9314 Cloud computing - ENISA Liaison Reports

PCI (Payment Card Industry) Council (2010) PCI DSS (Data Security Standard) Requirements and Security Assessment Procedures Version 2.0, OCTOBER 2009。

附件一　PlayStation Network 出包 可能洩漏 7700 萬人的個資

http://taiwan2ch.pixnet.net/blog/post/29881228#axzz1MX6DWImr

針對 Sony 的遊樂器 Play Station 3 等進行的網路非法侵入而對伺服器進行的攻擊，造成世界上有史以來最龐大的 7700 萬人的個人資訊流出問題，讓該公司的未來所籠罩的巨大烏雲越來越廣。

有人指出（華爾街日報），「有史以來最嚴重的資訊外洩」的代價會超過兩億日圓，甚至也無法避免到追及經營責任，該公司正面對著未曾有過的危機。

外洩的資訊包括姓名、地址、電子郵件帳號，生日、密碼等等。而該公司更是表示，信用卡的號碼有效期限也無法被排除外洩的可能性，所以呼籲用戶注意，就信用卡 的使用記錄上「希望能定期確認」。由於光是在日本的登錄者約有 900 萬人，是日本企業資訊外洩記錄有史以來最龐大的，賠償的金額也將會達到天價。

對 於IT犯罪非常了解的紀藤正樹律師說明:「損害賠償金額，是根據所外洩的資訊品質而有所變化。若是只有住處、電話號碼等這些基本資訊的話，1個人相當於 5000日圓到1萬日圓的程度，但是若是外洩的內容包括跟個人名譽相關的資訊的話，金額就會暴增。」他又指出:「以日本的美容關連企業的案子來說，被命令 一個人要賠3萬日圓。以這個例子來推算Sony的情況的話，可能會賠償超過2兆圓以上。」

被害者當中，也有很多美國人。雖然覺得若是被有 「訴訟國家」之稱的美國給控告的話，得要付出鉅額賠償金，但是紀藤氏卻說:「關於個人資訊外洩的損害賠償請求，在美國很少進行。」但假設就算沒有求償，但 是包括道歉在內的事後處理費用，單純以一個登錄者「不低於5000日圓以下」(IT相關人員)。以此金額為基礎來計算也將近要「花費」將近4000億日 圓。

另外，IT作家井上トシユキ先生則指出還有別的賠償發生的可能性:「因為線上服務停止，(使用者)使用虛擬貨幣進行的線上遊戲資料儲存若是失敗，也可能會被請求損害賠償。」

對 事業的影響也大到無法想像，讓遊樂器、電視機、行動終端設備等的硬體連接網路，電影、音樂、遊戲等發送數位內容的業

務，是 Sony 現在著力最多的戰略。主導這個業務，而被拔擢為下任社長候選人第一人選的是平井一夫副社長(50 歲)。作為對於以同樣的手法先行一步的美國 Apple 公司的對抗策略，不得不擴大網路戰略的重要時刻卻發生了個人資訊外洩的事件。大大打擊了消費者的信賴程度，事業規劃被迫從根本上進行修正。

此外，更嚴重的是對於該公司對於資訊公開的「態度」。該公司雖然從 21 號開始停止了 Play Station Network，但是其理由只以「系統障礙」來說明。直到 27 號才發表了資料外洩的消息。在這件事上也有這樣的聲音：「26 號的時候，發表了對抗 Apple iPad 的平板新商品，難道他們不是一開始就打算一直等到這個發表結束的時候公布嗎？」有人認為 Sony 比起用戶的安全，還是以自己公司的方便為優先。

附件二　Sony PSN 事件說明會重點摘要

在說明會開始前不久，根據姊妹站 Joystiq 得到的消息，Sony 會提供某些遊戲 / 軟體的免費下載、30 天免費 PlayStation Plus（原 PSN 會員）、30 天免費 Qriocity 服務作為初步的補償，大家最關心的信用卡萬一怎樣了，Sony 一方面表示目前沒有證據顯示有任何詐欺案跟此次事件有關，將來要是會有，則會跟使用者一個個接觸，一切以個案來處理；如果要取消 PSN 服務，Sony 的作法將會跟信用卡一樣，暫時沒有提出具體的賠償方案，只說會跟個別使用者接觸、協調。

而相關服務的恢復，將會在一週內陸續重啟，預計在一個月內會整個完成，Sony 在會中則是不斷表示未來會加強相關的安全性防護...詳細內容各位可以往下繼續閱讀。

關於 PSN 個資遭竊的經過，Sony 先做出了以下的簡單解釋：

日本時間 4/20，Sony 首次偵測到非授權的存取，在初步判斷對方是高手中的高手後，就立刻延請第二家資料安全公司進駐，來分析該入侵者以及其造成的影響，隨後就寄出信件來警告使用

者；事後則發現有很多資料被竊取，不過關於信用卡的資訊（卡號、到期日、帳單地址等），Sony 表示沒有證據顯示這些資料也被偷走，不過 Sony 方面目前也沒有確認是否有任何跟信用卡有關的詐欺事件發生，有任何消息會公告周知，據信他們可能也不很清楚。

平井一夫表示，Sony 已經在著手部屬新的安全措施，以避免未來發生類似的事件；將會在美國聖地牙哥的新資料中心安插更先進的安全性防護，從加強的外部侵入感應、自動軟體偵測、 資料加密層級提高等等相關的改善，另外也會多蓋幾道防火牆；另外 Sony 也提醒使用者，近期要仔細核對信用卡的相關資訊（包括帳單），並且更改所有的密碼，以及任何跟 PSN 帳號密碼相同的其他網路服務帳號密碼。Sony 還說他們會考慮替受影響的 PSN 用戶支付新 PSN 信用卡發行所需的費用，同時已經確定會提供 30 天的免費 PS Plus 會員服務、30 天的免費 Music Unlimited 服務（Qriocity），外加一些特定遊戲、軟體內容的免費下載；而整個 PSN 服務的恢復，預計會在一個月內完成。

以下為 Q&A 重點整理：

1. PSN 上面有約莫 1,000 萬筆的信用卡資料，不過目前他們無法確定是否有任何資料被偷走

2. 預計將在一週左右的時間內重起服務；針對重新發行信用卡、PSN / Qriocity 銷售下滑（停機）方面，可能會造成 Sony 的財務損失，但是確切的影響還需要進一步評估

3. 對於有多少人遭受影響，Sony 表示還在調查資料洩漏、遭竊的程度，目前 PSN 上面有約莫 7,800 萬個帳戶

4. 由於 SNEI（Sony Network Entertainment Inc.）主要是位在美國，因此現在也在跟 FBI 合作；目前關於實際資料洩漏的狀況，他們也無法說太準，只說他們並沒有發現入侵者進入某些資料的證據。

5. 關於這次為何會讓入侵者走進來，是否 PSN 存在一些受攻擊的甜蜜點？Sony 方面的回答，說這次被插的點，是一個已知的

漏洞，不過 SNEI 的管理人員並沒有注意到這點，他們目前已經在部屬相關的安管人員來進行改善。Sony 將會依照區域來一步一步進行信用卡監測的安全性防禦部屬。

6. 問到為何這麼久才跑出來開記者會：Sony 方面表示，發現問題的第一時間，他們就將 PSN 關閉，但分析相關資料需要時間，我們必須逐步來採取各項行動，而且我們一發現問題，就第一時間通知使用者；但是在關閉部分 PSN 服務，以及分析相關資訊的時間，的確花了他們比較多的時間；Sony 表示一開始他們有相當多的推測，但是並沒有任何證據顯示有人在此次攻擊事件後操盤，目前也還都是一些推敲而已；信用卡的資訊有受到加密，但是使用者的其他 資訊可能就沒有保護到；針對未來將強力仰賴 PSN 的 NGP，Sony 表示將會透過加強網絡服務與更積極與用戶聯繫，來喚回使用者的信任、信心。

7. Sony 表示他們一定要能夠保護自家的智慧財產權，透過相關的安全防護機制，我們能夠提供玩家好玩的遊戲，維持住這樣的生態；我們絕不希望自家的平台被這樣破壞。

8. Sony 作出一點小小的更正，PSN 的密碼並沒有被加密保護，只有被混雜與散列（hashed）處理

9. 關於個資的後續補償，特別是萬一出現信用卡相關的詐欺事件，Sony 該如何處理：Sony 表示這次釋出的免費服務、遊戲，跟信用卡都沒關係，因為目前尚沒有任何證據顯示有任何的信用卡詐欺事件跟此次的資料洩漏有關連，未來若是有相關的狀況出現，Sony 將會一例一例來跟使用者接觸、處理。

10. 又有現場的記者戳 Sony，就是要逼他們說出到底有多少人取消 PSN 帳號這件事，同時 Sony 將會怎樣處理這些使用者在 PSN 當中留下的虛擬貨幣、點數：Sony 的回答，跟信用卡一樣，將會一例一例來處理；他們說會盡可能以合理流程來進行相關退費、補貼，但是目前暫時還沒有具體的計畫。

http://chinese.engadget.com/2011/05/01/sony-psn-press-event/ 2011/5/12

附件三　北京市朝陽區人民法院審理王菲訴海南天涯線上侵犯名譽權案民事判決書

原告王菲，男，1980 年 5 月 26 日出生，漢族，無業，住北京市朝陽區武聖東裏*號樓*室。

委託代理人張雁峰，北京市京都律師事務所律師。

委託代理人董宇瓊，北京市京都律師事務所律師。

被告海南天涯線上網路科技有限公司，住所地海南省海口市濱海大道珠江廣場帝都大厦 10 樓 B 座。

法定代表人邢明，總裁。

委託代理人蘇雪映，女，1977 年 2 月 5 日出生，漢族，海南天涯線上網路科技有限公司職員，住海南省海口市龍昆南麓道客新村*巷*號。

原告王菲（以下簡稱姓名）與被告海南天涯線上網路科技有限公司（以下簡稱天涯公司）名譽權、隱私權糾紛一案，本院受理後，依法組成合議庭，公開開庭進行了審理。王菲的委託代理人張雁峰、董宇瓊到庭參加了訴訟，天涯公司的委託代理人蘇雪映經本院傳票傳喚，到庭參加了第一次庭審，未參加第二次及第

三次庭審。本案現已審理終結。

王菲訴稱：我與姜岩於 2006 年 2 月 22 日結婚。由於雙方性格差異大等原因，婚後感情不和，尤其是 2007 年 6 月我患病後雙方感情進一步惡化，2007 年 10 月雙方鬧起離婚。2007 年 12 月 29 日姜岩跳樓自盡。

2008 年1月10日,天涯公司註冊管理的天涯虛擬社區網(以下簡稱天涯網）中，出現了《大家好，我是姜岩的姐姐》一帖，該貼捏造事實，對我進行誹謗。眾多網友在跟帖時，使用了侮辱性語言，對我施行了“網路暴力”。網友還不斷重複地披露我和家人的隱私。天涯公司的行為給我和家人的生活、工作、名譽造成極為惡劣而嚴 重的影響：被騷擾、被單位辭退，其他單位也因之不敢聘用；父母住宅多次被人騷擾，門口兩側貼滿誣陷恐嚇標語；報刊、電視臺等多家媒體在報導姜岩死亡事件時 作出了對我極不公正的報導……

因此請求判令天涯公司立即停止侵害、刪除天涯網上有關侵權資訊，並在天涯網為我恢復名譽，消除影響，賠禮道歉，賠償精神損害撫慰金 2 萬元，賠償工資損失 4 萬元，承擔公證費用 2050 元的三分之一。

天涯公司辯稱：我公司天涯網上的資訊全部是由上網用戶發佈，並非我公司發佈，我公司不應成為本案被告。我公司在王菲起訴前及時刪除了天涯網上《大家好，我是 姜岩的姐姐》一帖及相關回復，已經履行了監管義務，不存在任何過錯，不應承擔侵權法律責任。根據《互聯網電子公告管理規定》、《互聯網資訊服務管理辦法》 及《資訊網路傳播保護條例》的規定，網站發現有侵權內容存在後及時刪除的，不應承擔共同侵權責任。根據《互聯網電子公告管理規定》，網站應對註冊用戶提示網站上發佈資訊需要承擔的法律責任。天涯網在用戶發帖或回復時都有相應的字體提示以及用戶在註冊時應當閱讀並同意的《天涯社區基本法》及其它相關社區規 則。因用戶言論導致的侵權責任，應由其自己承擔責任，我公司盡到了法定義務，不應承擔任何侵權責任。因此不同意王菲的訴訟請求。

經審理查明：王菲與死者姜岩系夫妻關係，雙方於 2006 年 2 月 22 日登記結婚。2007 年 12 月 29 日，姜岩從自己居所的 24 層樓高處跳樓自殺。

姜岩生前在網路上註冊了博客，並進行寫作。在自殺前 2 個月，姜岩關閉了自己的博客，但一直沒有中斷博客的寫作。姜岩

在博客中以日記形式記載了自殺前兩個月的 心路歷程，將王菲與案外女性東某的合影照片貼在博客中，認為二人有不正當兩性關係，自己的婚姻很失敗。姜岩的日記顯示出了丈夫王菲的姓名、工作單位位址等 資訊。姜岩在第一次自殺（2007 年 12 月 27 日）前將自己博客的密碼告訴一名網友，並委託該網友在 12 小時後打開博客。在姜岩第二次自殺（2007 年 12 月 29 日）死亡後，姜岩的網友將博客密碼告訴了姜岩的姐姐姜紅，姜紅將姜岩的博客打開。

天涯虛擬社區 （www.tianya.cn）是由天涯公司於 1999 年 3 月註冊的經營性網站。天涯網的簡介中介紹該網站註冊用戶近 2000 萬。該網站制定有《天涯社區 基本法》、《網站關鍵字過濾措施》等規定，根據這些規定，在對網友提交內容的監控方面，分為四級監控過濾，即重要敏感關鍵字監控、次要敏感關鍵字監控、一 般敏感關鍵字監控、敏感廣告詞監控。

姜岩的博客日記被一名網友閱讀後轉發在天涯網中，後又不斷被不同網友轉發至其他網站上，姜岩的 死亡原因、王菲的“婚外情”等情節引起越來越多網友的長時間持續關注和評論。許多網友認為王菲的“婚外情”是促使姜岩自殺的原因之一；一些網

友在進行評論 的同時，在天涯論壇、大旗網等網站上發起對王菲的“人肉搜索”，使王菲的姓名、工作單位、家庭住址等詳細個人資訊逐漸被披露；一些網友在網路上對王菲進行 謾罵；更有部分網友到王菲及其父母住處進行騷擾，在王家門口牆壁上刷寫、張貼“無良王家”、“逼死賢妻”、“血債血償”等標語。直至本案審理期間，許多互 聯網網站上仍有大量網友關於此事的評論文章。

2008 年 1 月 10 日，天涯網上刊出《大家好，我是姜岩的姐姐》一貼帖，該帖講述了姜 岩死亡事件的發展經過。王菲認為該帖中如下言辭構成了誹謗：“王菲正與死者的親人爭奪死者遺產”、“是王菲全家把她逼死的，東方恩納一直住姜岩婆婆家…… 當時，王菲的父親和王菲打完電話，她就跳了”。王菲認為網友的如下回復帖子構成了侮辱：“姜岩還被那畜生一家這樣刺激過！”，“這種家庭別在找事顯眼了， 找個洞自己瞭解了吧”、稱原告為“賤男”、“看那兩個鳥男女能否還好下去”、“媽的，跟這種人住的近簡直是侮辱了這片土地……從這裏滾出去！”；“他們配 不上‘人’這個詞吧”；“這男的一家都是人渣”；“強烈建議人肉搜索出王菲！王蕾！和他那老王

八爹”等。

審理中，王菲提出曾於2008年1月10日向天涯網進行投訴，要求刪除包括該帖在內的相關資訊，但就此事實未提供相關證據。

天涯網於2008年3月15日（王菲起訴前）將《大家好，我是姜岩的姐姐》及相關回復帖子刪除。對此，天涯公司向本院提供了用於記錄刪除資訊的《版主傳來的帖子及處理結果備案》表。王菲對該表的真實性未提出異議，只是表示該表不能證明天涯公司沒有侵權事實。

2008年3月11日，王菲委託北京市方圓公證處對天涯網、大旗網、“北飛的候鳥”網三個網站中與本案相關的帖子、回復等證據進行了保全，花費公證費2050元。

本案審理中，王菲承認與東某確實曾有“婚外情”。

2008年1月19日，王菲作為乙方與姜岩的父母作為甲方簽訂關於姜岩後事處理的《協議書》。該協定第三部分第1條內容為“對於婚後乙方的不忠行為及以後發生的不幸事件，乙方向甲方表示誠摯的歉意”。

另，王菲為了證實由於此事被工作單位盛世長城國際廣告有

限公司辭退而產生工資損失，向本院提供了工資清單及盛世長城國際廣告有限公司在《大家好，我是姜岩的姐姐》一帖中回復的帖子，內容為：“……在得知此事原委之後，公司即決定讓王菲、東方兩名員工暫時停止工作，以妥善處理此事。其後不久，他們二人即向公司提請辭職，公司已予批准”。王菲的工資清單顯示其 2007 年 12 月的月工資收入為 19300 元。

上述事實，有雙方當事人當庭陳述、相關網站網頁、被告刪除記錄表等證據在案佐證。

本院認為：我國《互聯網資訊服務管理辦法》及《互聯網電子公告服務管理規定》中規定，互聯網資訊服務提供者應當向上網用戶提供良好的服務，並保證所提供的信息內容合法。任何人不得在電子公告服務系統中發佈含有侮辱或者誹謗他人、侵害他人合法權益的資訊。電子公告服務提供者發現其電子公告服務系統中出現明顯屬 於上述資訊內容的，應當立即刪除，保存有關記錄，並向國家有關機關報告。天涯公司作為天涯網的管理者，應當對該網站中發佈的文章、帖子履行監管義務。

眾所周知，互聯網在我國正飛速發展。據有關部門統計，網友的人數已經超過了 2 億，互聯網正在超越傳統媒體，趨顯“第

一媒體”之勢。天涯網的論壇上每天都會有 大量網友留下海量資訊。天涯公司作為天涯網的管理者，依照相關法律法規和規定，制定有上網規則，對上網文字設定了相應的監控和審查過濾措施，達到了相應要 求；由於中國文字的豐富性、多樣性以及網路語言的不斷更新變化，網站事實上不可能將所有不雅言辭均納入監控範圍；根據目前現有的、通常的網站管理方式和技 術手段，網站的管理者也不可能對所有網友的全部留言進行事前逐一審查。因此，網站管理者的監管義務應以確知網上言論違法或侵害他人合法權益為前提，在確知的情況下如果放任違法或侵權資訊的存在和散播，則構成侵權；而及時履行了刪除義務的，不構成侵權。

天涯公司的監管義務應是在自行發 現或受害人投訴後及時將涉嫌侵權的資訊刪除或修改。王菲主張曾經向天涯網進行過投訴，因無證據佐證，本院無法采信。天涯公司在王菲起訴前將《大家好，我是姜岩的姐姐》一帖及相應回復刪除，已經履行了監管義務。鑒於互聯網具有的廣泛、迅速、即時、隨意、互動等傳播特點，天涯公司的這種事後刪除行為符合相關規 定，不構成侵權。因此王菲主張天涯公司侵犯名譽權、隱私權不能成立。王菲

基於天涯公司侵權提出的停止侵害、賠禮道歉、賠償工資損失、公證費及精神撫慰金等 請求本院不予支援。

綜上，依據《中華人民共和國民法通則》第一百零一條之規定，判決如下：

駁回原告王菲的全部訴訟請求。

案件受理費二百二十元，由原告王菲負擔（已交納）。

如不服本判決，可於本判決書送達之日起十五日內向本院遞交上訴狀，並按對方當事人的人數提出副本，交納上訴案件受理費，上訴於北京市第二中級人民法院。如在上訴期滿後七日內未交納上訴案件受理費，按自動撤回上訴處理。

（2008）朝民初字第 29277 號

發佈時間： 2008-12-18 14:39:27