雲端安全化及雲端鑑識化之新思維與新趨勢:
--雲端應用化，也要雲端安全化，更要雲端鑑識化

➢ 林宜隆 博士

中華民國電腦稽核協會(CAA)理事長

台灣數位鑑識發展協會(ACFD)理事長

元培醫事科技大學資訊管理系(數位創新管理碩士班)教授 兼

雲端服務與數位鑑識產業融合發展研究中心召集人

健康(醫療)雲端服務實驗室召集人

➢ @行政院資通安全會報資安技術交流小組顧問 / 委員

➢ @法務部調查局資通安全諮詢委員

➢ 中央警察大學資訊管理學系、研究所兼任教授

➢ 網路犯罪問題研究室總召集人

資通安全鑑識與犯罪問題研究室總召集人

➢ 中華民國資訊管理學會常務理事兼資通安全管理委員會主任委員

➢ 前台灣電腦網路危機處理暨協調中心TWCERT/CC執行長

➢ ISMS:BS7799/ISO27001 LA 主導稽查員

➢ ITSM: ISO20000 Auditor稽查員

➢ BCM: BS25999/ISO22301 LA主導稽查員

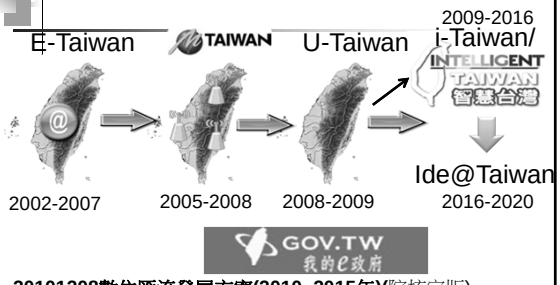
➢ PRMP:ISO29100 個資風險管理師

➢ PIISMS:ISO27018:2014 LA 雲個資保護稽核師

雲端安全化及雲端鑑識化之新思維與新趨勢:
雲端應用化，也要雲端安全化，更要雲端鑑識化
演 講 大 綱

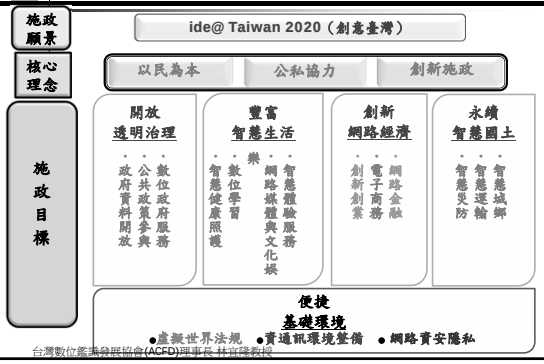
- **ide@ Taiwan 2020（創意臺灣）(2015-2020)數位國力**
- **What is the 資安鑑識四部曲 &** Forensic Computing? **(by Paul Lin & Jill Slay)**
- **What is the 4P's Model? (by Paul Lin & Jill Slay)**
- **What is the 6S of Service Models for Cloud Computing?(by Paul Lin)**
- **What is the DEFSOP**? **(by Paul Lin)**
- 雲端應用化，也要雲端安全化，更要雲端鑑識化
- Discussion of 4P's Model by Paul Lin & Jill Slay
- ACFD Demo

國家資通建設計畫進程(NICI)

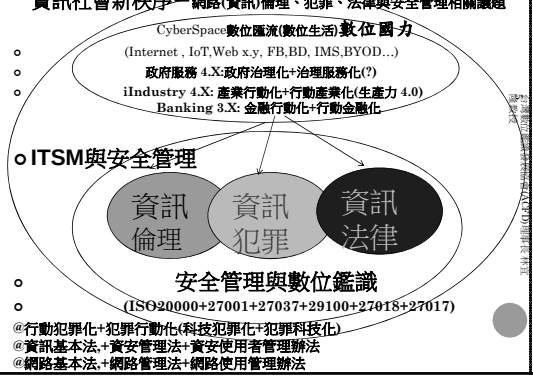


20101208數位匯流發展方案(2010~2015年)(院核定版)
20121004數位匯流發展方案（2010-2015年）第二版
20150702 ide@ Taiwan 2020（創意臺灣）(2015-2020)數位國力

20150702 ide@ Taiwan 2020（創意臺灣）(2015-2020)
施政願景(數位國力)



大數據時代:雲端安全化及雲端鑑識化之新思維與新趨勢:
雲端應用化，也要雲端安全化，更要雲端鑑識化
資訊社會新秩序—網路(資訊)倫理、犯罪、法律與安全管理相關議題



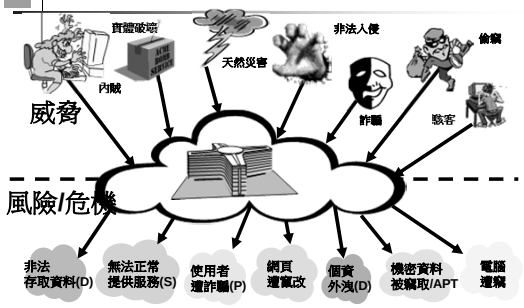
@行動犯罪化+犯罪行動化(科技犯罪化+犯罪科技化)
@資訊基本法,+資安管理法+資安使用者管理辦法
@網路基本法,+網路管理法+網路使用管理辦法

資安鑑識四部曲:
資安預防、資安防護、證據保全與專業鑑識
(CYBER FORENSIC & FORENSIC COMPUTING)

- 4Ps=Prevention + Protection+ Preservation +Presentation
- **=資安預防(P1)+資安防護(P2) +證據保全(P3)+專業鑑識(P4)**
- L1:Prevention: Firewall, IDS,IPS…..UTM
- L2:Protection:**資訊安全(密碼技術, DES, RSA, SHA, PKI…)病毒原理(Malicouse Code, AV, AS, AF, CF..)**
- L3:Preservation: ICT Auditing,**Cyber Forensics & Forsensic Engineering,** VM/PM
- L4:Presentation:DEFSOP, **CyberCrime & digital Crime**
- **@@5Ps= 4Ps+ Promotion (Paul Lin)**

雲端(資通)安全威脅與風險(犯罪)

RISK/CRISIS(Crime)=A*V*T

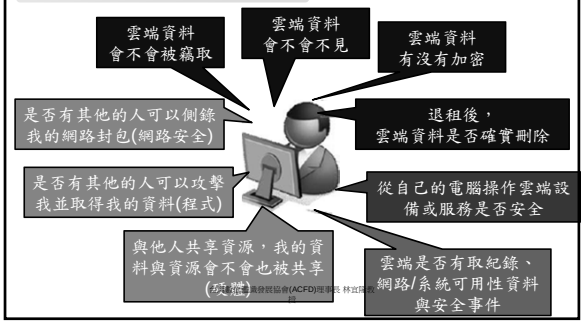


<<<DSP model by Paul Lin on 2008-2016>>>

從使用者(Auditing)角度看雲端安全風險

雲端安全風險之探討

從使用者(Auditing)角度看雲端



資通安全之迷思?

1.史上最嚴重個資外洩事件(2011/04)

PSN個資被盜 SONY恐賠7000 億

（編譯林冠廉／綜合報導）SONY的遊戲主機網路平台 PlayStation Network（PSN）遭駭客入侵，高達七千七百萬名用戶個資被盜一事，除了美國用戶提訴之外，歐洲的個資保護機構也要追究責任。日本產經新聞指出，若以過去日本判例，一人賠償三萬日圓的金額計算，SONY在這次被稱為「史上最嚴重個資外洩」事件中，賠償總金額恐將超過二兆日圓（約台幣七千億元）。

一名熟諳網路犯罪的律師紀睦正衡表示，個資外洩的損害賠償，依外洩的內容而異，住址、電話號碼、信用卡號等基本資料外洩的話，一人賠償金約五千到一萬日圓，但洩漏的內容若涉及個人名譽，金額又會不一樣。律師指出，日本曾發生過的類似企業個資外洩案，當時法院判賠每人三萬日圓，如果比照這個金額，SONY大概得賠二兆日圓以上才能了事。

- **Sony的遊戲主機服務網站PSN外洩7,700萬筆會員資料，2011/5月旗下影音娛樂網站也相繼淪陷，超過 1億筆會員資料外洩**
- **外洩資料包含用戶帳號、密碼、出生年月日、聯絡地址、電話、e-mail，甚至包含信用卡資料**
- **Sony公布1.71億美元的善後成本（僅事件通知處理費用），但風險評估單位Ponemon Institute推估Sony必須付出高達240億美元的善後損失及天價賠償**
- **民眾對Sony失去信心，各項影音娛樂、遊戲硬體、手機、平板電腦都下滑，股市下跌8%**

2.英電信商客戶400萬名個資外洩　駭客要求贖金

2015年10月24日03:16

- 英國電信及寬頻網絡供應商TalkTalk網站21日遭駭客入侵，數百萬客戶個人資料恐有外洩之虞。公司行政總裁哈丁23日說收到駭客要求贖金，已報警處理，並未透露贖金金額。
- TalkTalk估計約400萬名用戶的姓名、地址、電郵地址、生日、電話、信用卡號碼及銀行帳戶等個人資料面臨被竊風險。TalkTalk提供電話、寬頻上網和有線電視服務，這是它今年遭到已知的第3次攻擊，最新一次發生於21日，但TalkTalk直到22日晚上才通知客戶和警方，遭客戶炮轟。 有客戶投訴，帳戶內數百英鎊被人盜走，在她不曾逛過的網路商店付款。
- 當地警方目前仍未查出駭客身份，TalkTalk建議客戶留意帳戶是否有異常，並向信用評等機構查詢個人的信用資料。（國際中心／綜合外電報導）

2.少年駭客入侵電信公司,四百萬個資外洩

2015年10月27日18:40

- 英國倫敦警方表示，在北愛爾蘭逮捕一名15歲少年，涉嫌入侵英國電話及寬頻網絡供應商TalkTalk，竊取了逾400萬名當地客戶的個人資料。
- 警方在聲明中表示，周一(26日)下午搜查安特里姆郡(Antrim)一處住宅時，這名少年因涉嫌違反電腦濫用法遭逮捕，目前已經被帶到安特里姆警局拘留。
- 本月21日，TalkTalk遭到「顯著和持續的網絡攻擊」(APT)，上周末公司行政總裁哈丁(Dido Harding)形容，攻擊較早先預估來得「輕微」，但相信客戶個人資訊及銀行資料等資訊已經被盜取。不過被偷的銀行資料只是局部，並不足以提取金錢。
- 此次是TalkTalk在八個月來第三次被駭客入侵偷取客戶資料，TalkTalk表示，目前還不確定多少客戶受到影響。（於慶中／綜合外電報導）

3.聯發科前主管涉竊個資 起訴(1/2)

2015-10-29 04:48:50 經濟日報 記者謝佳雯／台北報導

- 聯發科人力資源部離職林姓女主管被控竊取內部人事資料案，昨（28）日遭到台北地檢署依妨礙**營業秘密和背信等**罪嫌，起訴林女及其丈夫。聯發科表示，將持續捍衛保護智慧財產與營業秘密。
- 檢方調查，林女曾在聯發科擔任人力資源管理專案副理，先生在聯發科擔任工程師。她在2012年離職前，涉嫌將內部的員工人事資料寄到自己私人電子郵件信箱。
- 檢方調查，這些員工資料包含專長、學歷、曾任職公司、現職、個人聯絡方式等，合計多達三、四千筆；為取得這些工程師的分機資料，還使用丈夫在聯發科的帳號密碼，登入人資系統查詢。
- 檢方調查，林女離職後開設獵人頭公司「艾特」，並利用手上的人事資料打電話回聯發科，為多家高科技公司高薪挖角，聯發科員工懷疑個人資料外流，內部著手調閱相關電腦紀錄和郵件後，因而提告。**(4P's Model)**
- 檢方調查，林女利用這些資料，親自或透過其他員工打數百通電話挖角，但並無所獲。雖然林女指稱，過去任職人力部門主管，因工作需要將員工資料存到私人電郵，離職後打電話到聯發科是找朋友聊天；她的丈夫也說，在家中登錄人資系統是因工作需要。
- 檢察官認為，兩人飾詞狡辯，決定將兩人起訴。

@聯發科指出，將持續保護智慧財產與營業秘密，內含產品研發秘密、人事與整體營運等秘密。

@過去八年聯發科共發生四件疑似營業秘密被竊案，多數是員工離職時帶走機密資料。為保護公司重要資產，內部共建立三個團隊，加上內部控制稽核，進行風險控管。

@@目前聯發科有三個單位聯手推動**智慧財產治理，包括政策制定與溝通、風險控管和稽核，所有離職員工還會透過內部電子簽核流程，確保機密資料沒被帶走**。【記者李淑慧／台北報導】律師表示，所謂營業秘密不見得一定是高科技技術，只要符合「具經濟價值、採取相當保密措施、未公開」三項條件，就是營業秘密。**(4P's Model)**

➢3.聯發科前主管涉竊個資 起訴(2/2)

聯發科去年三起狀告員工竊密案

被告對象	事件	附註
前高階主管袁帝文	聯發科懷疑其離職前複製大量機密資料，並跳槽競爭對手展訊	檢調偵辦中、袁帝文已至展訊任職
鑫澤和離職員工	聯發科十名員工跳槽鑫澤，懷疑帶走研發秘密	檢調偵辦中
前離職人資主管	聯發科認為其帶走機密人事資料，並另開人力仲介公司為客戶挖角	遭台北地檢署正式起訴

資料來源：經濟日報整理　謝佳雯／製表

經濟日報提供

@@資安議題 美企升至董事會層級

2014年07月01日 04:10記者洪紹運／綜合外電報導

- 華爾街日報報導，全美第二大零售商Target遭駭等資安問題連串爆發後，網路維安問題的防範已提高至企業董事會層級，不再只是科技專家的份內事。
- 其中，食品製造商家樂氏公司（Kellogg Co.）將該議題置入董事會議程中，重要性不亞於傳統議題，如穀物食品趨勢、零售商沃爾瑪（Wal-Mart）合作案等。
- 家樂氏高層擔心網路駭客會竊取其相關技術，例如家樂氏米花卡通人物的行銷手法，或是品客洋芋片的彎曲角度等。為防範駭客威脅，家樂氏董事會2012年成立網路維安專案小組，並首度聘用資訊安全長（Chief Information-Security Officer）一職。
- 另外，全球最大肉品供應生產商泰森（Tyson Foods）、石油公司艾克森美孚（Exxon Mobil Corporation）皆加強對維安議題之關注。2011年，達美航空（Delta Air Lines Inc.）董事會更加入資安背景的，以成員協助企業營運。
- 根據知情人士表示，早在去(2013)年Target公司遭駭客竊取4千萬筆信用卡、金融卡會員資料之前，沃爾瑪高層即經常收到來自顧問公司關於駭客威脅的報告，其中，就包括目標在竊取易付卡資料的俄羅斯駭客等。
- 華爾街日報分析師指出，**今(2014)年為止，已有1,517家於紐約證交所、那斯達克掛牌交易之企業，**將網路安全、駭客、網路攻擊、資訊破壞等相關議題，列入企業風險之一，遠**高於去(2013)年全年的1,288家及2012年的879家企業。**
- 然而，雖然資訊安全意識逐漸抬頭，但美國聯邦政府仍指出，部分企業依舊忽視其重要性。
- **@@公開發行資料 (將網路安全、駭客、網路攻擊、資訊破壞等相關議題，列入企業風險之一)(資安議題 美企升至董事會層級) (4P's Model)**

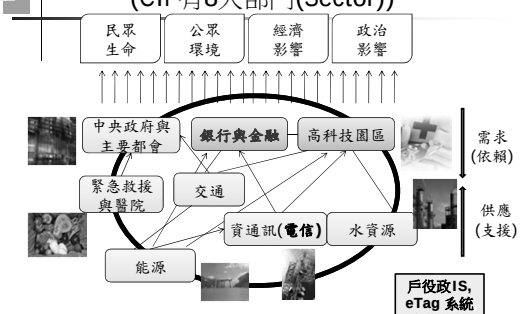
近期CIIP/CIP重大資安威脅事件(2013)

- 民國102年2月25日內湖麗源大樓IDC業者「數位通」位於其機房內的機電設施發生異常及損壞造成火災，**大樓供電因消防滅火安全而斷電**，導致全臺9成對外海纜網路服務，以及諸多網站、網路服務被迫中斷12個小時以上(CIIP/CIP)
- 民國102年3月20日國安局長蔡得勝20日在立院公布驚人數據，國安局外網網域，過去1年遭駭客入侵、攻擊高達334萬次，等於**平均每天就要承受1萬次的攻擊(CIIP/CIP)**
- 民國102年3月20日南韓爆發南韓史上最大駭客攻擊，多家銀行、保險公司、電視臺和電信網路業者，遭受大規模駭客攻擊，對外服務中斷，**受害電腦數量高達3萬2千臺(CIIP/CIP)**
- 民國**102年4月25日與 11月03日及12/15**高鐵又跳電, 影響3.2/2.9萬人, 其不合格危機處理能力及發生原因調查. (CIIP/CIP 含數位鑑識)

近期CIIP/CIP重大資安威脅事件(2014-2015)

- eTag, 戶役政系統, 台鐵(CIP/CIIP)
- 台鐵在1030228當天發生史上最嚴重的電車斷線事件,影響六萬人以上旅客(CIP).
- 新戶役政系統103年2月5日上線後，經持續改善雖已漸趨穩定，但仍有部分跨機關通報資料異常、無法即時通報等問題，內政部續督促廠商儘速調校修正。為全面體檢新一代戶役政資訊系統，已邀請專業顧問、資訊中心及相關軟硬體廠商緊急成立專案小組，以儘速解決新系統不穩定之技術面問題。(CIIP/CIP)
- 遠通eTag日前(103/1/1)正式上路，用路人抱怨連連，指稱系統連番扣款錯誤，高公局在過年前祭出「全民監督國道通行費計畫」，要全民揪錯。遠通電收坦承，3日、4日有上百輛車的eTag重複扣款，發現是系統調教時出問題，覆核後已將誤扣金額補還客戶。
- eTag、戶役政更可說是「**日日與民同呼吸」的資訊系統(CIIP/CIP)**；亦即，民眾對這些系統有蟲、出包的忍受度，本就遠低於其他系統。官員若未周密沙盤推演、預先設想十八套因應劇本，即有疲怠之虞。

我國關鍵基礎建設(CI)部門 (CIP有8大部門(Sector))



資料來源：行政院國土安全辦公室民國100年CIP委外研究期末報告

資通安全之迷思?

COMMON ATTACK TYPES(2006~2016)

- Virus(Malware), APT(Sony Playgame)
- Spyware(ex.96.03.30軍機頻外洩 中國看光光)
- Phishing (personal)+資料外洩DLP
- Spam mail (personal)

(完整郵件治理解決方案首重-過濾與稽核+證據保全)

- Unauthorized Access (如個資外洩)
- DoS/DDoS(Botnet)
- **Cloud Securit**y+Cloud Computing
- Mobile & Wireless **Security**
- Forensic Computing (4P's Model by Paul Lin & Jill Slay)
- **Cloud Forensics+ Mobile Forensics**
- **CIP+CIIP+Cyber Warfare**
- **行動犯罪化+犯罪行動化(科技犯罪化+犯罪科技化)**
- **產業行動化+行動產業化，(產業犯罪化+犯罪產業化)**
- **政府服務4.0+政府治理化+治理服務化(?) , COBIT 5.0**

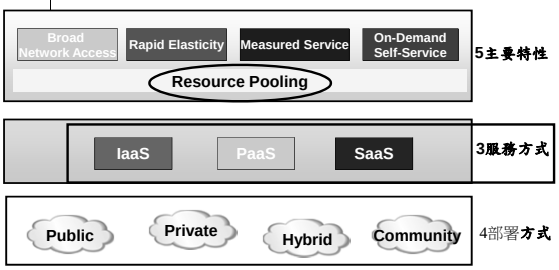
[網路犯罪(Cybercrime,CC)]的質變

- **過去CC 1.0**
  - 個人
  - 展示技術能力、出名
  - 隨機找尋目標
- **現在CC2.0**
  - 集團或組織化(黑道、天幫商人等)
  - 獲取金錢利益(19 歲駭客年收入百萬)
  - 堅持入侵特定目標，不達目的不罷休(中共網軍)
  - 逃避偵測(Slow attack)與反監控
- **多種新型態犯罪，在網路世界上演真實犯罪CC 3.0**
  - 網路色情、盜版、網路詐騙
  - 竊取機密資料或虛擬寶物、DDoS恐嚇勒索、綁架資料、操控殭屍電腦部隊、幫派搶地盤等, Botnet, 網路釣魚(Cyber Phishing)
  - 社交工程,網路釣魚,個人資料外洩, APT...etc
- **網路跨國犯罪因法令、管轄權因素，難以追查及起訴(電信詐欺,網路詐欺,網路購物,社交工程,個資外洩...etc)**

@目前資安威脅趨勢與資料外洩 (DSP model by paul)

- **資料竊取、資料洩漏(DLP)**
- **針對性攻擊**
- **主要目的為獲取金錢**
- **具特定目標的惡意程式攻擊來竊取機密資料**
  - 使用者瀏覽惡意網站而被植入惡意程式（標的主要為**網路銀行**和線上遊戲）
  - 點選惡意電子郵件和即時訊息內所含的URL連結時，會連結上惡意網站
- **網路犯罪CC4.0標的DSP:資料(Data)+服務(Service)+特權(privilege).....by Paul Lin**
- **Banking 3.0:** 金融行動化+行動金融化
- **行動犯罪化+犯罪行動化(科技犯罪化+犯罪科技化)**
- **金融卡詐欺手法與防範(165.gov.tw)**

美國NIST對雲端運算的定義

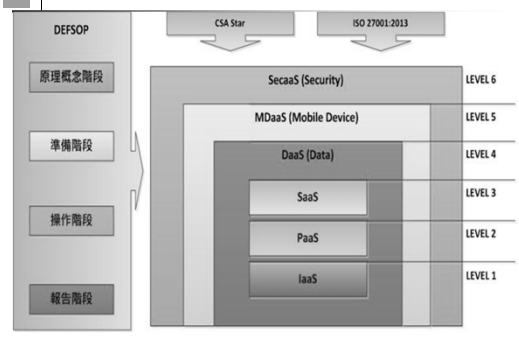


Source: Cloud Security Alliance (Dec. 2009), Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

雲端運算的組成

- **三個服務模式3S（Service Models）------4S-----5S---6S**
  - **雲端軟體**（SaaS：Software as a Service）
    - 在雲端提供**應用軟體租賃**，由使用者依需求決定要使用的範圍以及付費標準。
    - 例如：Dynamic CRM Online、Office Online或其他公司的商用軟體。
  - **雲端平台**（PaaS：Platform as a Service）
    - 在雲端中的**軟體技術支援**，用以開發雲端應用軟體或服務。
    - 例如 Windows Azure Platform、SQL Azure、AppFabric。
  - **雲端建設**（IaaS: Infrastructure as a Service）
    - 在雲端的**硬體運算資源與管理支援**，通常由雲端大廠提供機房或是切割的特別領域供使用者運用。
    - 例如：主機服務 (Hosting)
  - **雲端資料庫**(DaaS：Database as a Service)
    - Data Base servers
  - **雲端安全**(SaaS：Security as a Service) and**雲端行動**(MaaS: Mobile Devices as a Service)

iCC-DEFSOP雲端運算之架構(by Paul Lin)

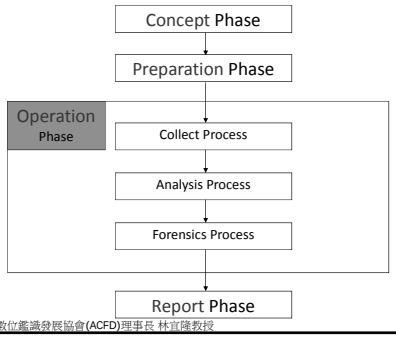


雲端運算的組成

- **八種共通特性**（Common Characteristics）
  - **海量級擴充性**（Massive scale）
  - **同質性**（Homogeneity）
  - **虛擬化**（Virtualization）(VM)
  - **快速且彈性的運算能力**（Resilient computing）
  - **軟體低成本**（Low cost software）
  - **地理分布**（Geographic distribution）
  - **服務導向**（Service orientation）
  - **進階安全技術**（Advanced security technologies）(ISO/CSA/ENISA)
  - ✓ ISO/IEC 27017 will cover **information security controls for cloud computing.**
  - ✓ ISO/IEC 27018:2014 cover **privacy aspects(PII) of cloud computing.**
  - ✓ ISO/IEC 27014:2013 offers guidance on the **governance of information security.**

The DEFSOP architecture:

digital evidence forensic standard operating procedure



What is the Operational phase of DEFSOP?

- In the operational phase, this phase is consisted of three parts, collect process, analysis process, and forensics process.
- proposed cloud digital evidence forensics standard operating procedure on VoIP to resist several attacks from cloud security threats. (DEFSOP for VoIP,2011, on JDI,SCI)
- In regarding to digital evidence technology, the major property is to preserve, identify, distract, record and interpret the computer and network system evidence, through complete and perfect methods and procedures.

The 4P model consists of prevention, protection, preservation and presentation(by JILL Slay,2007). Lin(Paul Lin) defines cloud digital evidence forensics standard operating procedure denoted by Cloud-DEFSOP. The corresponding relation between 4P model and Cloud-DEFSOP model is shown in Fig. 2.

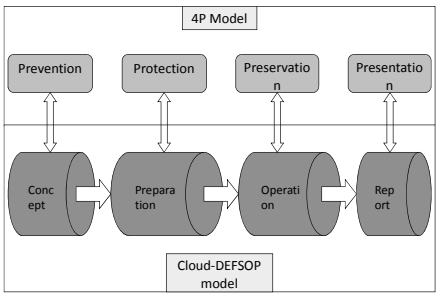


Figure 2. Forensics mapping function of 4P model and Cloud-

CSM資通安全管理面(Cyber Security M.)

- **技術導向：**
  1. **資訊安全(密碼技術,DES,RSA,SHA,PKI…)**
  2. **病毒原理(Malicouse Code,AV,AS,AF,CF..)**
  3. **網路安全,防火牆(FW),UTM**
  4. **入侵偵測系統（IDS） -> 入侵預防系統IPS**
  5. **駭客攻/防技術(Hacking),**
  6. **Secure Code and Secure SE(SSE/SSDLC)**
  7. **Cyber Forensics & Forsensic Engineering**
  8. **弱點評估&弱點分析&滲透測試(VA&VA&PT) nessus,**
  9. **APT, Mobile Security, Cloud Security,**
  10. **IoT security, App Security….**
- **管理導向：(含ISO20000/ISO27001/ISO29100/ISO27018)**
  1. **網路管理與資通安全管理與認知**
  2. **SP,SM,SA, USM**
  3. **駭客攻/防策略與管理**
  4. **電腦稽核& ICT Auditing**
  5. **風險管理&風險評鑑(RM&RA)(ISO27005)**
  6. **垃圾郵件(Spam mail)之管理(Email Auditing)**
  7. **ISP連線管理(IPP,IAP,ICP)**
  8. **VM,PM,SRM(ISO27005),ERM**
  9. **CyberCrime & Digital Crime(ISO27037)**

(資安措施實務)個人資料保護法施行細則(民國 101 年 09 月 26 日)行政院通過

(公務及非公務機關之適當安全維護措施(PLSE model))

第十二條 本法所稱適當安全維護措施、安全維護事項或適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，**採取技術上及組織上之必要措施。**

前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有**適當比例為原則**：(PLSE model)

- 一、配置管理之人員及相當資源。
- 二、界定個人資料之範圍。 **(個資盤點)**
- 三、個人資料之**風險評估及管理機制**。(RM)
- 四、事故之預防、通報及應變機制。(IR)
- 五、個人資料蒐集、處理及利用之**內部管理程序。(IPO model)**
- 六、資料安全管理及人員管理。
- 七、認知宣導及教育訓練(Awareness)。
- 八、設備安全管理。
- 九、**資料安全稽核機制(DB auditing)。**
- 十、**使用紀錄、軌跡資料及證據保存。(DEFSOP)**
- 十一、個人資料安全維護之整體持續改善。(BCM:BS25999/ISO22301)

適當的安全防護措施

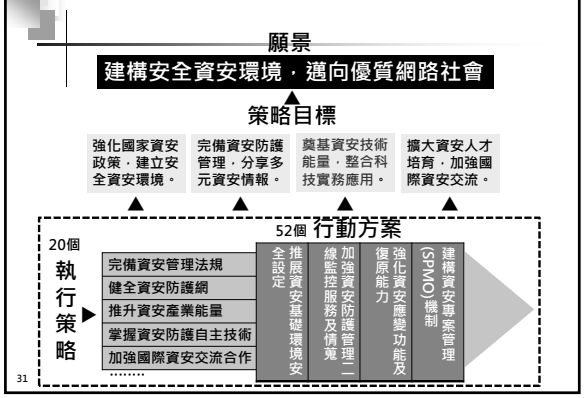
證據保全與數位鑑識

從使用者(Auditing)角度看雲端安全風險

雲端安全風險之探討

從使用者(Auditing)角度看雲端

@國家資通訊安全發展方案概述(102-105)106-



重要執行策略與行動方案(3/4)

目標	執行策略	行動方案	主辦單位	協辦單位
目標三 奠基資安技術能量，整合科技實務應用。	3.1. 掌握資安防護自主技術	3.1.1.建構資安防護技術研究能量	國科會、經濟部、國防部	資通安全辦公室
		3.1.2.推動資安防護技術整合應用	經濟部、國安局、資通安全辦公室	
	3.2. 加強網路犯罪偵查能量	3.2.1.強化網路犯罪偵查科技應用	內政部、法務部	資通安全辦公室
		3.2.2.建置網路犯罪偵查整合性「知識庫」	內政部、法務部	資通安全辦公室
	3.3.建立數位證據保全及鑑識能量	3.3.1.完善數位證據保全及相關標準作業程序	法務部、內政部	資通安全辦公室
		3.3.2.研議建立數位鑑識實驗室驗證制度	法務部、內政部	資通安全辦公室
	3.4. 強化軟體安全管理	3.4.1.建置國家軟體資產控管機制	資通安全辦公室	各機關
		3.4.2.推動「安全軟體發展生命週期（SSDLC）」	資通安全辦公室	科技會報辦公室、各機關
	3.5. 建構政府行動化安全機制	3.5.1.建構政府行動軟體(APP)安全檢測機制	資通安全辦公室	研考會
		3.5.2.規劃政府行動化安全防護機制	資通安全辦公室	研考會
		3.5.3.提升政府無線網路安全措施	資通安全辦公室	研考會

ISO 27001資訊安全管理系統簡介

ISO 新編號	原標準標號	名稱
27000		Vocabulary and Definitions
27001	BS7799-2 ISO 24743	ISMS Requirement Specification
27002	BS7799-1 ISO 17799	Code of Practice of ISMS
27003	ISO 24742	ISMS Implementation Guideline
27004	-	ISMS Metrics & Measurement
27005	BS7799-3	ISMS Risk Management
27006	-	Guidelines for information and communications technology disaster recovery services

ISO27011 for **telecommunications organizations(電信產業)**
ISO27015 **for financial services organizations**. **(金融產業)**
ISO27799 for Health care **(health sector)(醫療產業)**
ISO27037 for **digital evidence (數位證據)**

http://www.iso27001security.com/index.html

雲端安全與數位鑑識偵查標準

- ISO/IEC 27017:2015 will cover **information security controls for cloud computing.**
- ISO/IEC 27018:2014 covers **PII (Personally Identifiable Information) in public clouds.**

ISO/IEC 27037:2012 covers **identifying, gathering and preserving** digital evidence(DEFSOP)

ISO/IEC 27041:2015 guideline on assurance for digital evidence investigation methods.(SOP)
ISO/IEC 27042:2015 guideline on analysis and interpretation of digital evidence.(證據能力)
ISO/IEC 27043:2015 guideline on digital evidence investigation principles and processes. (證據能力與證明力, 證據有效性)

美國對數位鑑識能量的投入

施行沙賓、Basel II法案 ⇨ 數位鑑識為公司風險管理之重要基礎 ⇨ 國際四大會計師事務所均已成立相關部門

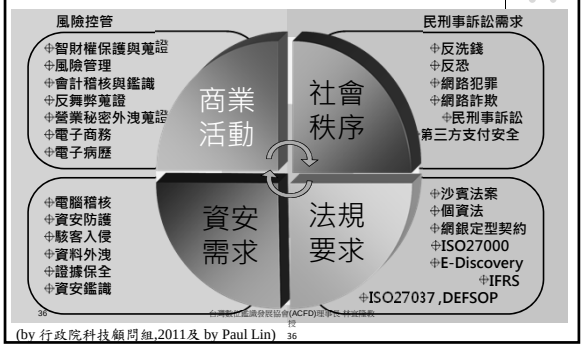
FBI數位鑑識實驗室(RCFL)
2002年6個→2010年16個(by paul Lin)
開放民間公司實驗室承辦鑑識工作

E-discovery(2006.11)
電子蒐證(發現)法
處理不當會左右訴訟成敗

- ✓打擊網路犯罪
- ✓強化數位鑑識能量與執法人員訓練
- ✓建立SOP/DEFSOP

數位鑑識需求領域

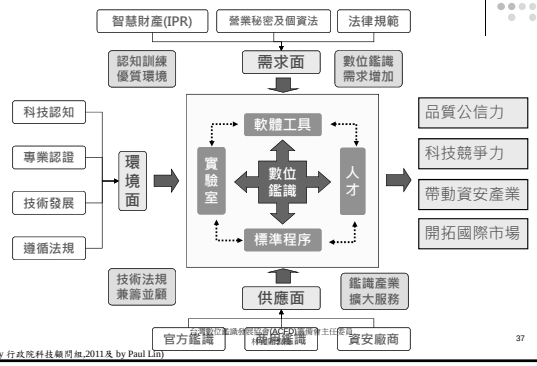
@(資安鑑識能量=ICT(Lab.)+SOP+專業(國際證照)人才, by Paul Lin)
@數位鑑識是以科學方法與合理程序，對數位證據進行保全、採證、分析及呈現科學



(by 行政院科技顧問組,2011及 by Paul Lin) 36

我國數位鑑識發展規劃

(資安鑑識能量=ICT(Lab.)+SOP+專業(國際證照)人才, by Paul Lin)



(by 行政院科技顧問組,2011及 by Paul Lin)

資安專業人才

- 資安防護人才(Q/Y, UNIT,Contents)
- 資安攻擊人才
- 資安鑑識人才**(ACE/EnCE/CFCE/UCE/CFE)**
- 資安偵查人才**(CFCE/CFE)**
- 資安教育人才(ISO27001/27011 LA)
- 資安治理人才(ISO27014)

數位鑑識(資安鑑識)

(Computer Forensics, Cyber Forensics)

(Warren G. Kruse ii and Jay G. Heiser, 2002, *Computer Forensics – Incident Response Essentials*, Addison Wesley)

The IPCC Model by Paul Lin(1995/2012)

- 定義：(資通安全鑑識)
  - 以周延的方法及程序保存, 識別, 抽取, 記載, 及解讀電腦及網路媒體證據與分析其成因之科學
- 方法與基本原則:(IAC+C) (CIA)(CIAC)
  - 在不改變或破壞證物的情況下取得原始證物**(I完整性**)
  - 證明所抽取的證物來自扣押的證物**(A正確性**)
  - 在不改變證物的情況下進行分析**(C一致性)**
  - **採用符合法律及法規的程序進行證物鑑識(C適法性)**

(Albert J. Marcella Jr. and Robert S. Greenfield , 2002, **Cyber Forensics- A Field Manual of Collecting, Examining, and Preserving Evidence of Computer Crimes**)

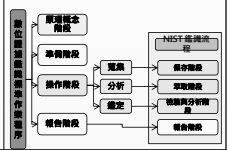
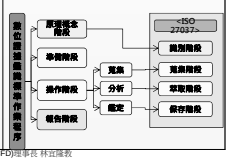
數位鑑識標準作業程序(DEFSOP)比較分析

作者	程序
Kuchta (美國學者)	1. 準備工作 (Preparation) 、 2. 文件紀錄 (Documentation) 、 3. 收集 (Collection) 、 4. 鑑定 (Authentication) 、 5. 分析 (Analysis) 、 6. 保存 (Preservation) 、 7. 結果 (Production) 、 8. 報告 (Reporting)
Kruse & Heiser (美國學者)	1.保存證據、2.檢驗證據、3.案件分析與陳述、4.呈現結果
林宜隆 (國內學者) DEFSOP	1.原理概念階段(原則、法規、認知) 2.準備階段(授權、安全政策、確定人事時地物、準備工具、資料探勘) 3.操作階段 (蒐集、分析、鑑定) 4.報告階段(撰寫、呈現驗證、法庭準備、建檔學習)

※綜合專家學者對數位鑑識程序的觀點，並歸納出數位鑑識流程不外乎有下列幾點：準備工作、搜尋、保存、復原、分析、檢查、鑑定及呈現結果。

參考資料：司法新聲101期第4篇數位證據鑑識標準作業程序（DEFSOP)與案例實證之研究

數位鑑識標準作業程序(NIST/ISO27037)比較分析

國際標準	程序	與DEFSOP對應關係
美國國家標準技術局 NIST	1.保存階段 (Preservation) 2.萃取階段 (Acquisition) 3.檢驗與分析階段 (Examination and Analysis) 4.報告階段 (Reporting)	
ISO 27037	1.識別階段 (Identification) 2.蒐集階段 (Collection) 3.萃取階段 (Acquisition) 4.保存階段 (Preservation)	

參考資料：司法新聲101期第4篇數位證據鑑識標準作業程序（DEFSOP)與案例實證之研究/International Standard, 2012/10/15,ISO/IEC 27037

CLOUD FORENSICS FRAMEWORK

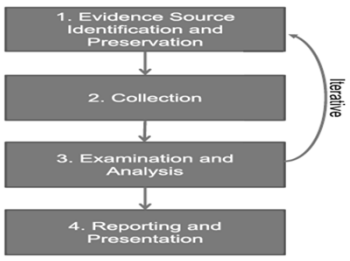


Fig. 1. Cloud forensics framework.

Cloud storage forensics: ownCloud as a case study

Ben Martini*, Kim-Kwang Raymond Choo
Information Assurance Research Group, School of Information Technology & Mathematical Sciences, University of South Australia, GPO Box 2471, Adelaide, SA 5001, Australia

Digital Investigation 10 (2013) 287–299

The DEFSOP architecture:

digital evidence forensic standard operating procedure

- Concept Phase
- Preparation Phase
- Operation Phase
  - Collect Process
  - Analysis Process
  - Forensics Process
- Report Phase

DEFSOP數位鑑識的有效性(CIAC)
(4P's Model)

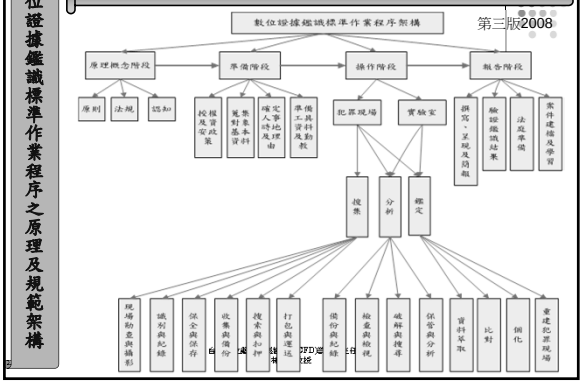
DEFSOP	4P's模型	有效性 適法性	完整性	正確性	一致性	說明
原理概念階段	預防 (Prevention)	V				C:採用符合法律及法規的程序進行證物鑑識
準備階段	防護 (Protection)		V			I:在不改變或破壞證物的情況下取得原始證物
操作階段	保全 (Preservation)			V		A:在不改變證物的情況下進行分析
報告階段	呈現 (Presentation)				V	C:證明所抽取的證物來自扣押的證物

※每個階段都包含有效性；但每個階段各有強調的功能

台灣數位鑑識發展協會(ACFD)籌備會主任委員
林宜隆教授
參考資料：司法新聲101期第4篇數位證據鑑識標準作業程序（DEFSOP)與案例實證之研究(林宜隆)

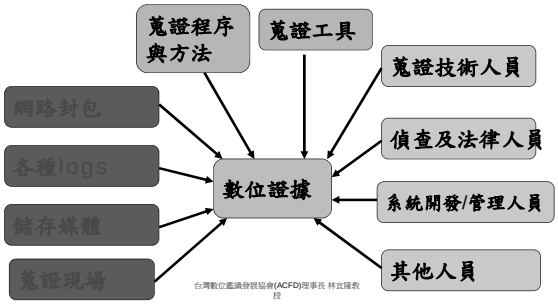
數位證據鑑識標準作業程序之原理及規範架構

第三版2008



數位證據蒐證相關構面

The CF Model by Paul Lin(1995/2012)



資安鑑識四部曲:
資安預防、資安防護、證據保全與專業鑑識
(Cyber Forensic & Forensic Computing)

- 4Ps=Prevention + Protection+ Preservation +Presentation
- **=資安預防(P1)+資安防護(P2) +證據保全(P3)+專業鑑識(P4)**
- L1:Prevention: Firewall, IDS,IPS.....UTM
- L2:Protection:資訊安全(密碼技術,DES,RSA,SHA,PKI…)病毒原理(Malicouse Code,AV,AS,AF,CF..)
- L3:Preservation: ICT Auditing,Cyber Forensics & Forsensic Engineering, VM/PM
- L4:Presentation:DESOP, CyberCrime & digital Crime
- **@@5Ps= 4Ps+ Promotion (Paul Lin)**

對個資法實施之因應策略
--數位證據保全與數位鑑識
(4P'S MODEL BY PAUL LIN & JILL SLAY)

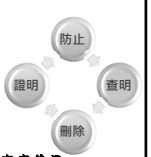
Prevention 資安預防	Protection 資安防護	Preservation 證據保存	Presentation 專業鑑識
事前	事中	事後	

✓風險評估與管控
- 公務機關(將個資納入ISMS認證)
- 非公務機關(ISMS認證、TPIPAS認證、電子商務交易安全作業基準等)

✓人員認知教育
✓個資的存取權限控管與監控機制、資料外洩防護DLP
✓資安聯防及通報應變機制
✓數位證據保存(DEFSOP)

舉證免責
✓數位證據力
✓證據能力

風險分擔
✓個資保險



民事損害賠償專業基準

The 4p's Model by Paul Lin(1995/2012)

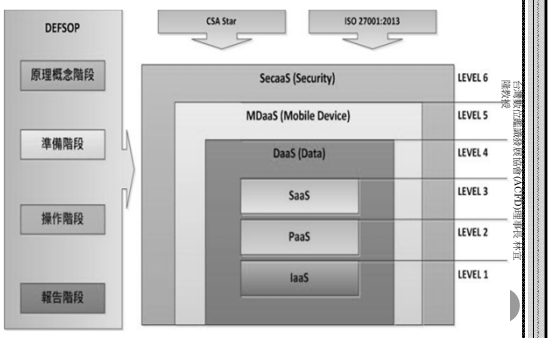
(ISO27001+ISO27037+ISO29100+27018)=PIPM+PIPA

資安鑑識能量=Cyberlab.(ISO17025)+SOP(ISO27037)+鑑識人才(ISO17024)

@建立整合式雲端威脅之數位證據鑑識標準作業程序雛形(iCC-DEFSOP)

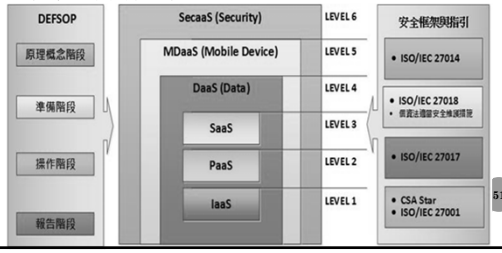
- 除了NIST所提出的IaaS、PaaS、SaaS三層之外，另外再加上DaaS(Data as a Service)、MaaS(Mobile Device as a Service)以及SaaS(Security as a Service)三個層級[11]，共六個層級.(by Paul Lin)
- 此六個層級各掌控不同的控制項目，運用PDCA循環，除了以國際認證標準之安全ISO27001:2013、CSA Star CCMv1.4控制措施加以控管(ISO27017+27018)，並套用林宜隆教授(Paul Lin)所提出之DEFSOP，提出一套符合現況雲端架構。(iCC-DEFSOP)

- iCC-DEFSOP雲端運算之架構(by Paul Lin)



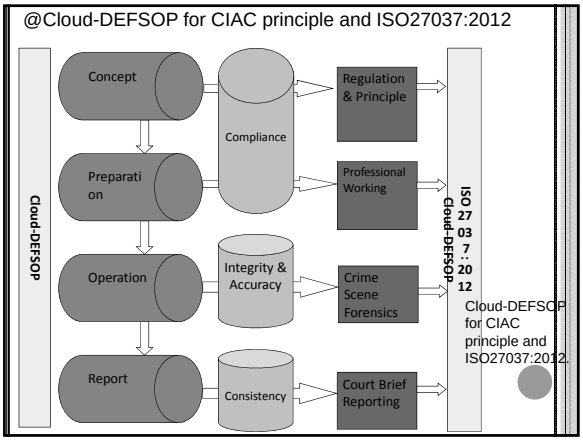
建構整合式雲端威脅之數位證據鑑識標準作業程序雛形

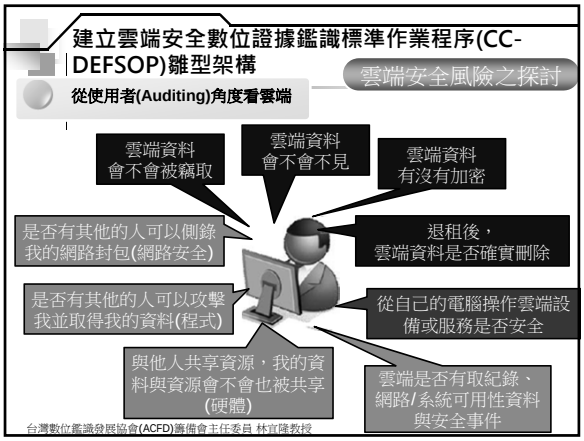
- NIST所提出的IaaS、PaaS、SaaS三層，再加上DaaS(Data as a Service)、MaaS(Mobile Device as a Service)以及SaaS(Security as a Service)三個層級所對應之IS0/IEC 27017、IS0/IEC 27018、IS0/IEC 27014，並套用林宜隆教授所提出之DEFSOP，提出一套符合現況雲端標準作業程序雛形.



- 建立整合式雲端威脅之數位證據鑑識標準作業程序（iCC-DEFSOP）

DEFSOP	Could Level		雲端服務	ISO 27001:2013	CSA Star CCMv1.4	PDCA
原理概念階段	Level6	SecaaS	雲端安全數位鑑識與防護 雲端服務治理 雲端資安檢測	A.5資訊安全政策 A.6資訊安全的組織 A.8資產管理 A.14資訊系統取、開發與維護 A.15供應者關係 A.18法律與契約要求事項之遵循性	1.遵循性 5.資訊安全 6.法令 9.營佈管理 11.安全架構	P(Plan)
準備階段	Level5	MDaaS	雲互連	A.5資訊安全政策 A.8人力資源安全 A.13通訊管理 A.18法律與契約要求事項之遵循性	4.人力資源 5.資訊安全	D(Do)實
操作階段	Level3	SaaS	雲市集 雲端應用軟體	A.5資訊安全政策 A.9存取控制 A.10密碼 A.11實體與環境安全 A.12運作管理 A.16資訊安全事件管理 A.18法律與契約要求事項之遵循性	3.設施安全 5.資訊安全 8.風險管理 10.復原力	C(Check)
	Level2	PaaS	創作平台 元件服務 視覺營效平台 巨量資料運算			
	Level1	IaaS	虛擬運算 虛擬網路 虛擬儲存			
報告階段	Level4	DaaS	雲端儲存	A.5資訊安全政策 A.17營運持續管理之資訊安全層面 A.18法律與契約要求事項之遵循性	2.資料管制 5.資訊安全	A(Action)





建立雲端安全數位證據鑑識標準作業程序(CC-DEFSOP)雛型架構

雲端安全風險之探討

從CSA角度看雲端

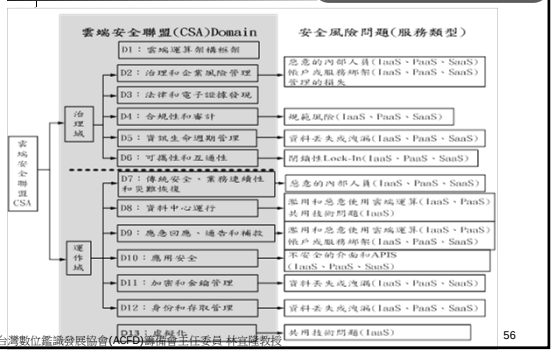
雲端的治理方式 Governance Domains	雲端的運作方式 Operational Domains
治理和企業風險管理	傳統安全、業務連續性和災難恢復
法律和電子證據發現	資料中心運行
合規性和審計	事件回應、通告和補救
資訊生命週期管理	應用安全
可攜性和互通性	加密和金鑰管理
	身份和存取管理
	虛擬化

cloud security alliance

虛擬化為雲端安全中之全新領域

建立雲端安全數位證據鑑識標準作業程序(CC-DEFSOP)雛型架構

雲端安全風險之探討



建立雲端安全數位證據鑑識標準作業程序(CC-DEFSOP)雛型架構

雲端安全標準規範探討

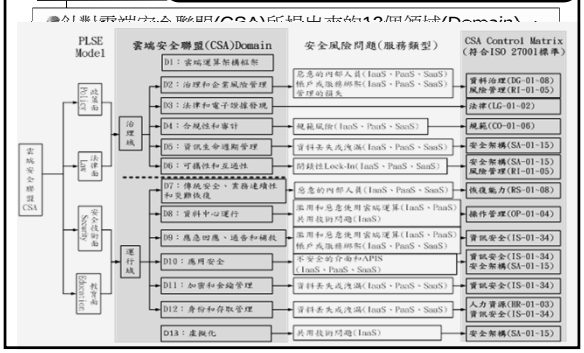
雲端安全聯盟(CSA)制定了一套叫做雲端控制模型（Cloud Controls Matrix，CM）的基本安全規範，開發出一套針對雲端服務進行安全性評估的公開問題集，共有11大項安全規範控制區；98項安全規範控制ID，其規範對映標準如下：

- COBIT(Control Objectives for Information and related Technology)

Control Area	Control ID	Compliance Mapping				
		COBIT	HIPAA	ISO/IEC 27002-2005	NIST SP800-53	PCI DSS
Compliance - Audit Planning	CO-01		HIPAA 164.312(b)	ISO/IEC 27002-2005 15.3.1	NIST SP800-53 R2 CA-7 NIST SP800-53 R2 PL-6	
Compliance - Independent Audits	CO-02	COBIT 4.1 DS5.5	HIPAA 164.308 (a)(8)	ISO/IEC 27002-2005 6.1.8	NIST SP800-53 R2 CA-2 NIST SP800-53 R2 RA-5 NIST SP800-53 R2 CA-6	PCI DSS v1.2 11.2 PCI DSS v1.2 11.3
Compliance - Third Party Audits	CO-03		HIPAA 164.308 (b)(2)(iii) HIPAA 164.308 (b)(4)	ISO/IEC 27002-2005 6.2.3 ISO/IEC 27002-2005 10.2.1 ISO/IEC 27002-2005 10.2.2	NIST SP800-53 R2 CA-3 NIST SP800-53 R2 SA-9 NIST SP800-53 R2 SC-7	PCI DSS v1.2 2.4 PCI DSS v1.2 12.8 PCI DSS v1.2 12.8.1 PCI DSS v1.2 12.8.2 PCI DSS v1.2 12.8.4
Compliance - Contact / Authority Maintenance	CO-04			ISO/IEC 27002-2005 6.1.6 ISO/IEC 27002-2005 6.1.7		
Compliance - Information System Regulatory Mapping	CO-05			ISO/IEC 27002-2005 15.1.1		
Compliance - Intellectual Property	CO-06			ISO/IEC 27002-2005 15.1.2	NIST SP800-53 R2 SA-6 NIST SP800-53 R2 SA-7	

建立雲端安全數位證據鑑識標準作業程序(CC-DEFSOP)雛型架構

雲端安全數位證據鑑識標準作業程序雛型



未來資通安全及數位鑑識新知識與新科技

- Hacking and Attack/Defence Strategy
- Secure Code / Secure SE
- Cybercrime and CyberForensics CC 4.0
- Digital Evidence and Cyberevidence
- Cybercriminology(如MOP理論, 情境犯罪預防理論)CC 4.0
- Cyberlaw
- ISMS(ISO17799:2005/BS7799/CNS17799/17800/ISO27001:2005)+ISO27037+ISO27041-43
- ITSM(ISO20000); BCM(BS25999/ISO22301);PRMP:ISO29100
- Cyber Security Management and Governace(ISG/CSG)
- CISA/CISM/CGEIT/CRISC for ISACA by Pass ISO17024
- Cloud Computing and Cloud Security/Forensics(**雲端服務與安全管理)ISO27017+27018**
- **資安鑑識能量=Cyberlab.(ISO17025)+SOP(ISO27037)+鑑識人才(ISO17024)**
- **金融行動化+行動金融化， 金融犯罪化+犯罪金融化，行動犯罪化+犯罪行動**

數位鑑識偵查能量

- **數位鑑識偵查能量=Lab.(Tools)+ SOP(執法SOP)+專業人才**
- **如何建置符合國際標準的數位鑑識實驗室及工具**
- **如何建構數位鑑識的SOP及方法論(DEFSOP)**
- **如何培育數位鑑識的專業證照人才(EnCE, ACE,UCE)**
- **資安鑑識能量=Cyberlab.(ISO17025)+SOP(ISO27037)+鑑識人才(ISO17024)**
- **i- SOC**
- **=ISMS(ISO27001)+ITSM(ISO20000)+BCM(ISO22301)+PIPM(ISO29100/ISO27018)+DE(ISO27037)by Paul Lin**

未來網際網路新知識與新科技
=cybercrime+cyberforensics+cyberlaw
（=網路犯罪+電腦鑑識+資訊法律）
(cyber2011研討會:100年11月25~26日)
主題:雲端安全服務與個人資料保護
http://www.ypu.edu.tw/cyber2012/
(cybre2012研討會:101年12月26日)
主題: CIIP與個人資料保護
http://www.ypu.edu.tw/cyber2013/
(CIIP研討會:102年03月29日)
主題: 國家資安發展與CIIP推動
(cyber2013研討會:102年11月22~23日)
主題:鑑識會計與個人資料保護
http://cyber2013.conf.tw/
(cyber2014研討會:103年12月5日)台北商業大學
主題:雲端服務應用、安全與稽核
http://cyber2014.ntub.edu.tw
cyber2015研討會:104年10月24日
主題:（大數據時代:智慧健康生活與行動安全服務及隱私權保障）
http://cyber2015.chihle.edu.tw
cyber2016研討會:105年11月18-19日大同大學
主題:**新引擎:翻轉資安科技、創新服務與風險管理**

台灣數位鑑識發展協會(ACFD)

(Association of Cyber Forensics Development, ACFD)

- 各位先進，大家好：

  感謝各位先進的支持，
  @發起人暨第一次籌備會已於10月28日（三）圓滿結束，
  會議中節錄重要決議如下：（會議記錄如附件）
- 由林宜隆、柴惠珍、盧公民、楊期蕊、萬幼筠、許林舜、呂芳際、許建隆、黃溶澤、許太千等10人為籌備委員，負責辦理籌備期間準備工作，並經全體委員共同推選並**通過由林宜隆委員擔任籌備會主任委員**。
- 籌備期間: 暫以台北市基隆路一段143號2樓之2為聯絡地址。
- 籌備期間重要議程預訂時程如下：
- **登報公告徵求會員：預於10月30日（星期五），並於12月10日（星期四）截止申請。**
- **成立大會暨第一次會員大會： 已於12月27日（星期日）早上9時30分，**
- **在台北市信義區基隆路一段143號2樓之2召開。**
- 並請準時與會，謝謝!

  聯絡人 許太千
-

  ACFD 網站 https://sites.google.com/site/taiwanacfd/
  ACFD facebook https://www.facebook.com/groups/462641917199704/
  ACFD e-mail acfdservice@gmail.com

台灣數位鑑識發展協會(ACFD)

ACFD FB: https://www.facebook.com/groups/462641917199704

台灣數位鑑識發展協會(ACFD)

ACFD 網站 : https://sites.google.com/site/taiwanacfd/
ACFD e-mail: acfdservice@gmail.com

- 恭喜元培醫事科技大學林宜隆教授當選<台灣數位鑑識發展協會(ACFD)>第一屆理事長，宜蘭大學趙涵捷校長當選第一屆常務監事，並聘任長庚大學許建隆教授為本會第一屆秘書長。
- 且經大會通過聘請行政院 張善政(副)院長為榮譽理事長，及聘任立法院 吳育仁委員，國立臺北商業大學 張瑞雄校長，中華民國資訊軟體協會 邱月香理事長，基隆港務警察總隊 金浩明總隊長，中華民國資訊管理學會 翁頌舜理事長，程曦資訊整合公司張榮貴總經理，國巨公司負責人朱瑞陽律師等為本會顧問。
- 104/12/27,台灣數位鑑識發展協會(ACFD,)成立大會，圓滿成功，是大家一起努力成果，也是歷史里程碑，未來必配合國家資安政策與鑑識科技及科技部國家資安科技中心，**共同達成國家資安防禦研發與產業發展**，更需要大家給本會指導及支持，再接再厲，感謝，感恩，感動

一月號刊出之ACFD成立新聞
CIO IT經理人雜誌
http://www.cio.com.tw/magazine/index.html ?
施鑫澤 <corey.shih@cio.com.tw> 於 2016年1月6日

行政院 張善政(副)院長為榮譽理事長1041227

台灣數位鑑識發展協會(ACFD)全體理監事1041227

台灣數位鑑識發展協會(ACFD)發展核心與目標

本會(ACFD)為推動台灣數位鑑識**政策、市場、人才及應用**的**標準化、產業化、專業化與創新化**，廣納國內外產官學界專業人士，協助國內「數位鑑識」發展為目標，俾與國際接軌。其未來**發展核心與目標**，如下:

1.**一核心價值**:**形塑政府及民眾對數位鑑識正確認知。**
2.**二個主軸**:**提升資安技術能量，健全數位鑑識防禦能量。**
3.三大構面:市場及產業，法規及政策，人才及技術。
4.四大應用化:數位鑑識應用**標準化，專業化，產業化，創新化。**
5.**五大目標**:**政策落實，法規健全，人才培育，產業紮根，應用創新**。

ACFD logo

ACFD 主 logo

ACFD 副 logo