2012 年第 2 季資訊安全管理系統標準化系列討論會：雲端運算環境之資訊系統安全授權規範－根基於 2011-12-08 美國聯邦政府公布之要求(FedRAMP: Federal Risk and Authorization Management Program)的實作

為持續配合行政院國家資通安全會報推動國內各政府機構及公民營事業機構建置資訊安全管理系統(ISMS)，以降低我國整體資訊安全風險，強化資訊防衛能力；經濟部標準檢驗局(BSMI)，自 91 年起每季 1 次辦理「堅實我國資訊安全管理系統稽核作業相關標準系列討論會」。原行政院「堅實我國通資訊基礎建設安全機制計畫」(90 年 1 月 17 日行政院第 2718 次院會通過)歷經 8 年共 2 期計畫後，於 98 年 1 月更名為「國家資通訊安全發展方案(98 年至 101 年)，簡稱資安發展方案」持續推動我國資安工作，前述討論會亦繼續辦理。

九十年代全球文明歷經了重大的轉變，品質、環境和職業安全衛生管理逐漸朝向一致化與標準化，而相關的國際標準也影響了許多國家經濟的發展和組織管理與經營的方式，ISO 9000 品質管理和 ISO 14000 環境管理系列標準的遵循，就是最佳的佐證。2000 年 12 月 1 日，資訊安全管理系統(ISMS)控制措施之 ISO/IEC 17799:2000(E)公布，2002 年 12 月 5 日相對應之 CNS 國家標準正式頒布，建立 ISMS 並擴大推動驗證已成為資訊安全之工作項目的主軸之一。2006 年 6 月 16 日，標準檢驗局再公布了 ISO/IEC 27001:2005(E)之資訊安全管理系統的驗證等國家標準，也成就了資安管理制度與國際化完全接軌的開端。

「讓過去與現在爭執不下，將錯失未來」，ISO/IEC JTC1/SC27 主席 Walter Fumy 先生，在世界資訊高峰會之邀請下，於 2004 年 09 月 24 日公布了 ISO 之深度防禦(Defense in Depth)的資訊安全管理模型觀點；其標準組件 ISO 27001 標準系列之 ISO/IEC 27003 已於 2010 年 2 月 1 日正式發行，ISMS 標準化的第一階段工作已樹立第 1 座里程碑。

標準可以累積知識與經驗，標準化則是冀求以系統的、共同的、協調一致的方法來強化標準實作的知識以供傳承。鑑於管理系統日益增多，其標準系列宜加以規範，國際標準組織(International Standardization for Organization，簡稱 ISO)自 2000 年起即分 3 階段進行管理系統標準(Management System Standards，簡稱 MSS)之標準化工作，期能在第 3 階段(2011~2015 年)完成各個管理系統要求事項的調合，ISO/IEC 27001 標準系列已遵循 MSS 逐步建立中，並納入雲端運算安全規範之議題。

研究「標準」的人是需要有「同情」與「推理」兩種能力，所謂「同情」是指「標準」的制定者要有對等之情，那樣體驗的「標準」自然是立體、多元的；「同情」加上「推理」，則「標準」是活的，每一份「標準」的頒布是因或是果，是趨勢或是成績，「標準」的產生絕非偶然而是無數之努力的形成。「標準」從長遠的角度來看，便可以體察出是有一股流勢，有無法阻擋的推移力量；資訊安全的「標準」更需要整合自然科學及社會科學之脈絡來解讀以及推理，才能溶入文化與數位台灣混然為一體，雲端運算標準化的進程僅為一端。

自 2002 年起，美國聯邦政府即致力於創建 ISMS 驗證機構之合規性要求，2011 年 12 月 8 日，在經過 24 個月的工夫後，根基於已建立：「以富於可操作性之精確性，在資訊安全攻防的片斷中，呈現反應與回復之脈絡」的連續性稽核之基礎上，正式公布雲端運算環境的資訊系統安全授權規範 FedRAMP (Federal Risk and Authorization Management Program)；ISMS 之標準化提供了一項建立與維持管理系統時得以遵循的模型，此 ISMS 模型(ISMS 標準系列)的特色仍包含了資訊安全領域中各專家所達成的共識，FedRAMP 將成為進行中之雲端服務安全標準化的 ISO/IEC 27017 系列標準與 ISO/IEC 27036-5 的源池。此次討論會(101 年 4 月 11 日)在行政院資通安全辦公室之指導下，由經濟部標準檢驗局與環奧國際驗證有限公司共同主辦，以前述標的之「發展與維護政府機關資安作業規範與參考指引」等重要措施行動方案的執行要點中之 ISMS 實作的議題規劃，希望對 ISMS 之落實提供正面助益，誠摯的歡迎您參加。

■ 時間：中華民國 101 年 4 月 11 日（星期三）

■ 地點：臺北市濟南路一段 4 號（經濟部標準檢驗局大禮堂）

■ 時程表

08:55~09:15	報到
09:15~09:25	開幕致辭
09:25~10:35	雲端服務的安全管理與個人資料保護相關標準初探 主講人：環奧國際驗證有限公司　陳昇智經理
10:35~10:50	休息
10:50~12:00	雲端運算(Cloud Computing)之安全評鑑與授權－根基於 FedRAMP (Federal Risk and Authorization Management Program) 主講人：中華電信股份有限公司電信研究所　單懷靈博士
12:00~13:30	午餐（供應便當）
13:30~14:40	雲端運算之資訊系統安全與供應鏈風險管理初探：根基於 ISO/IEC 1st CD 27002:2011-12-19 與 ISO/IEC 2nd WD 27017:2012-01-20 第 10 節 主講人：國立交通大學資訊管理研究所　樊國楨博士
14:40~14:55	休息
14:55~16:05	美國雲端運算供應商驗證機構遵循標準(ISO/IEC 17020/CNS 14725:2003-04-08)分析 主講人：全國認證基金會　石兆平副處長

■ 名額：100 名(以報名先後排序)。

■ 報名表：

資訊安全管理系統標準化系列討論會(101 年 4 月 11 日)

報 名 表

服務單位名稱			
學員姓名 (身份證號碼)	(　　)	(　　)	(　　)
註：公務人員欲經由本局登錄終身學習護照者請自行留下身分證字號，否則免留身分字號！			
地　　址			
聯絡人		電　　話	
傳　　真		E - m a i l	
用　　餐	□葷　　□素　　（請擇一打勾）		

※注意事項：

- 一律以 E-mail 報名：iso.service@bsmi.gov.tw 或 janeth@mail.tcicgroup.com。
- 請於討論會前一週(4 月 4 日前)完成報名手續，以便行政作業進行。
- 討論會通知將於討論會前 3 個工作天以電話或 E-mail 方式聯絡學員；討論會前一天若未接獲通知，請主動與標檢局王書薰小姐[電話：02-2343-4501]或環奧國際驗證有限公司洪嘉妤小姐[電話：02-2726-0262 ext.: 131]聯絡，以確保您的權益。
- 為響應政府限用紙杯的環保政策，請自備環保水杯，現場將提供開水。

- **指導單位：**
  行政院資通安全辦公室

- **主辦單位：**
  經濟部標準檢驗局
  環奧國際驗證有限公司

- **承辦單位：**
  中華民國檢測驗證協會