2015 年第 1 及第 2 季資訊安全管理系統標準化系列座談會：關鍵基礎設施資訊防護(Critical Infrastructure Information Protection，CIIP)與資訊安全管理系統(Information Security Management System，ISMS) － 雲端運算服務安全管理標準化(2015-03-31)以及《基於 ISO/IEC 27002 之能源公共工業過程控制系統資訊安全管理指南，ISO/IEC TR 27019：2013(E)》的修訂(智慧電網 ISMS 控制措施)建議(2015-04-01)

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(Information Security Management System，簡稱 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 9 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一座里程碑。

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 Organization for Standardization，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；已正式納入 ISO 之強制性規範(Procedures specific to ISO)，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，並納入關鍵基礎設施防護與個人資料保護管理系統安全規範之議題。

隨著政府機關對資通安全的重視，我國整體資安防護體系之建立與資安防護能力之提昇已見初步成效；2013 年行政院資通安全稽核作業計畫於 2013 年 9 月 2 日至 10 月 31 日，正式將「資安健診」的資訊安全技術項目控制措施之實作納入評分， 開啟我國資訊安全管理系統(Information Security Management System，簡稱 ISMS)稽核工作的新姿；「居安思危，思則有備，有備無患，敢以此規」，已納入「2013 年資訊安全重點工作項目」的年度政府機關（構）資通稽核作業 40%之「資安健診」的工作項目，開啟我國資訊安全管理系統（Information Security Management System，簡稱 ISMS）技術項目稽核之新頁，惟於 ISMS 的 ISO/IEC 27000 標準系列中之 ISO/IEC 27006 的附件 D，規範技術控制與系統測試的範疇已超越之；此外，在 2011 年已公佈之相關標準（ISO/IEC 27007 與 ISO/IEC TR 27008）宜參考，俾規範「資安健診」的標準化作業。

2013 年 12 月 25 日公布之「國家通資訊發展方案(102 年至 105 年)」第 2.2.4 項行動方案：「研訂 CIIP 基準」，我國正進行中的「雲端運算」與「智慧電

網」之關鍵基礎設施，ISO 已公布的「公共雲之個人資料保護的 ISMS 控制措施(ISO/IEC 27018：2014-08-01)」及根基於 ISO/IEC TR 27019：2013-07-15 進行修訂之「智慧電網 ISMS 控制措施」均與前述「研訂 CIIP 基準」的行動方案相關；根基於此，此次座談會(104 年 3 月 31 日至 104 年 4 月 1 日)在「行政院資通安全辦公室」之指導下，由「社團法人台灣網路防護協會」與「環奧國際驗證有限公司(TCIC)」共同主辦，分別以 「雲端運算服務安全管理標準化」及「基於能源公共工業過程控制系統資訊安全管理指南(ISO/IEC TR 27019：2013-07-15)的修訂(智慧電網 ISMS 控制措施)」建議等議題規劃，希望對 CIIP 之 ISMS 的落實能提供正面助益。「他山之石，可以攻玉」，此次會議承海峽對岸提供我國尚待開展的諸如美國雲端優先之 FedRAMP、工業控制系統現場測控設備(IEC 62443-4-1)、國際認證論壇(International Accreditation Forum，簡稱 IAF) 於 2015-05-26 要求 ISMS 稽核應具備的能力(ISO/IEC TR 27008)之標準化成果(GB/T 報批稿以及相關資訊等)及其講義供與會者參考，並由主辦單位安排專人(林國水教授、羅德興教授等)解說，囿於法規等原因，此次會議改為座談會方式辦理。

➢ **研討會時間與地點**

✧ **時間**：中華民國 104 年 3 月 31 日（星期二）

及 104 年 4 月 1 日（星期三）

✧ **地點**：臺北市基隆路一段 155 號 3 樓之 9

✧ （財團法人台灣網路防護協會會址）

時　程　表(預訂)

時間	104 年 03 月 31 日（星期二）	104 年 04 月 1 日（星期三）
08:55~09:20	報到	報到
09:20~10:35	「車聯網及隱私防護(ISO/IEC 29191：2012(E))」 講座：中華電信研究院 魏銷志博士	「工業控制系統現場測控設備安全功能要求：ISO/IEC TR 27019：2013(E)宜連結之現場測控設備(例：智慧電錶(Smart Meter))的安全功能要求標準」 講義： 中國國網智能電網研究院 高主任 昆侖博士 林國水教授研讀說明
10:35~10:45	休息	休息
10:45~12:00	「雲端運算之公共雲擴增的資訊安全控制措施(ISO/IEC 27018：2014(E))」 講座：環奧國際驗證有限公司 陳昇智經理	「車聯網驗證：智慧電網宜參考之具體而微的 ISO/IEC 27001：2013(E)ISMS 驗證要求事項標準」 講座：環奧國際驗證有限公司 梁日誠總裁
12:00~13:25	午餐（供應便當）	午餐（供應便當）
13:25~14:40	「雲端運算(云計算)服務安全管理制度及相關標準」 講義： 中國信息安全研究院有限公	「中國大陸 ISMS 稽核(审核)及資訊(信息)安全等級保護測評標準介紹：ISO/IEC TR 27019：2013(E)宜闡明之 ISMS 控制措施稽核的稽核

	司 左副院長 曉棟博士 羅德興教授研讀說明	員技能之要求事項標準」 講義： 北京時代新威信息技術有限公司 王總經理 新杰先生 樊國楨教授研讀說明
14:40~14:50	休息	休息
14:50~16:05	「從 Google 支援 FIDO U2F 雙因子(two factor)驗證(authentication)看物聯網之安全議題」 講座：奧樂科技股份有限公司 王基旆 總經理	「 ISO/IEC TR 27019 ：2013(E)修訂建議討論會」 引言(15 分鐘)： 台灣網路防護協會 樊國楨 博士

■ 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

服務單位名稱			
學 員 姓 名			
註：公務人員欲登錄終身學習護照者，於報到時請自行留下身分證字號。			
報 名 場	□104 年 3 月 31 日（星期二） □104 年 4 月 1 日（星期三）		
地 址			
聯 絡 人		電 話	
傳 真		E-mail	
用 餐	□葷 □素 （請擇一打勾）		
註：為因應新版個資法頒佈施行，特以此同意書，保障報名者接收相關訊息的權益：(請勾選) 本人□同意／□不同意，透過 e-mail/傳真/郵寄/電話接收本局及其他主/承辦單位相關訊息， 如：電子報/研討會/各類課程/及其他活動。非常感謝您的支持！			

※注意事項：

- 一律以 E-mail 報名：jin@mail.tcicgroup.com。
- 請於討論會前一週(3 月 23 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 TCIC 朱豫瑾小姐(電話：02-2726-0262ext123)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：**
  臺灣網路防護協會
  環奧國際驗證有限公司(TCIC Ltd.)
- **協辦單位：**
  奧樂科技股份有限公司