2023年第2季資訊安全管理系統標準化系列討論會:「資通安全管理法驗證方案特定要求」之標準化_根基於ISO/IEC 27001:2022(E)及ISO/IEC 27009:2020(E)

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(106年僅於第3季辦理1次1天, 107年僅於第1季及第3季辦理2次2天, 108~111年均僅於第1季辦理1次1天) ;因BSMI組織工作調整, 106年起改由「臺灣網路協會」辦理。

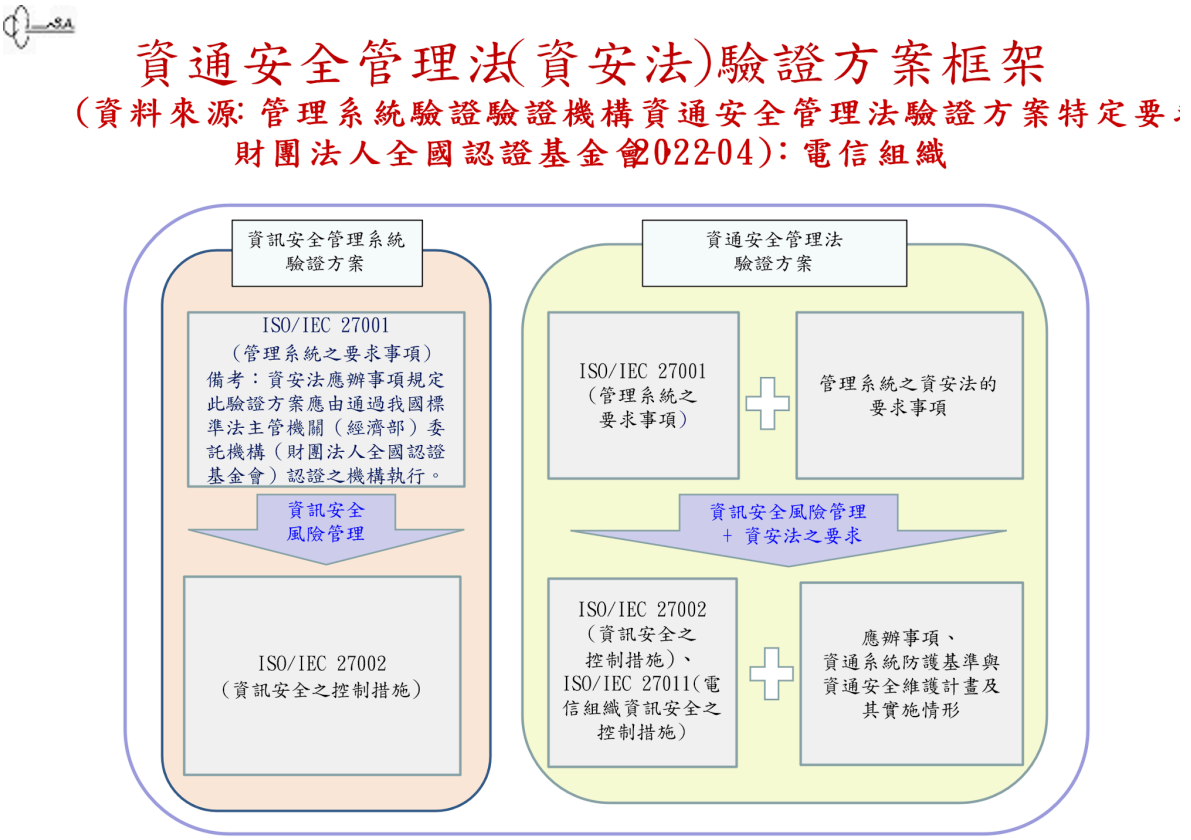
九十年代全球文明歷經了重大的轉變, 品質、環境和職業安全衛生管理逐漸朝向一致化與標準化, 而相關的國際標準也影響了許多國家經濟的發展和組織管理與經營的方式, ISO 9000品質管理和ISO 14000環境管理系列標準的遵循, 就是最佳的佐證。2000年12月1日, 資訊安全管理系統(ISMS)控制措施之ISO/IEC 17799:2000(E)公布, 2002年12月5日相對應之CNS國家標準正式頒布, 建立ISMS並擴大推動驗證已成為資訊安全之工作項目的主軸之一。2006年6月16日, 標準檢驗局再公布了ISO/IEC 27001:2005(E)之資訊安全管理系統的要求事項等國家標準, 也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;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, 並納入個人資料/隱私(Privacy)管理系統(PIMS)安全規範之議題;以個人資料保護法施行細則第17條之規範為例, 已公布ISO/IEC 27009、ISO/IEC 29101、ISO/IEC 29191、ISO/IEC 20008與ISO/IEC 20009標準系列, 作為其PIMS中「前檯匿名、後檯實名」之實作要求事項的參考。2012年10月, ISO/IEC JTC 1/SC 27在進行為期1年之2階段的研究後, 正式公布PIMS之要求事項遵循ISO/IEC 27001, 同時開展其標準系列(ISO/IEC 27009、ISO/IEC 27017、ISO/IEC 27018、ISO/IEC 27701、ISO/IEC 29101、ISO/IEC 29134、ISO/IEC 29151以及預備文件(SD 4等)的標準化計畫, 已於2017年8月完成第1階段之工作項目;並分成「管理」、「實作」與「技術」3個面向, 進行第2階段的標準制訂之計畫。

研究「標準化」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。「標準化」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「標準化」更需要整合自然科學、社會科學與資訊社會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, MSS與個人資料保護標準化及ISMS&PIMS, 以及網宇空間安全的整合性之資訊安全管理系統(Integrated Security Management System, 簡稱ISMS)的進程僅為一端。**於ISMS標準系列, 因涉及各國法規及日益增加之控制措施需求, 2013-02-07, 國際標準組織**(the International Organization for Standardization, ISO)**正式立項進行擴增**ISO/IEC 27001**與**ISO/IEC 27002**的規範供需用者採用以制定所需標準的**ISO/IEC 27009**之標準化計畫, 並於**2016**年6月16日發行;2019年8月5日, 遵循**ISO/IEC 27009**框架的**Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines**之:**ISO/IEC 27701**發行。2022年7月28日, **資訊安全, 網宇安全及隱私防護之資訊安全管理系統:要求事項**, Information security, cybersecurity and privacy protection — Information security management systems – Requirements :ISO/IEC 27001已於2022年10月25日發行, 開啟ISMS第3階段之標準化的工作項目。

繼2013年9月2日至10月 31日，「行政院國家資通安全會報」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ISMS稽核工作的新姿，並納入2013年12月15日「國家資通訊安全發展方案（102年至105年）」的「行動方案」之中；2022年5月1日，全國認證基金會已實施於2022年4月頒佈的《管理系統驗證機構資通安全管理法驗證方案特定要求》，開展我國資訊安全管理系統(Information Security Management Systems, ISMS)實作及其驗證的新頁，下圖為其電信組織遵循ISO/IEC 27009之框架示意說明。



1111109_資安法驗證框架ppt © TEJ(KJF)　　p14

10年歲月，「資安發展方案(110年~113年)」已分別推動「政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)」及「零信任網路(Zero Trust Network, 簡稱 ZTN)」中，均與ISO/IEC 27001：2022(E)直接相關；根基於此，此次討論會(111年11月30日)在國家安全局及數位發展部資通安全署之指導下，由中華電信股份有限公司、臺灣檢驗科技股份有限公司、台灣經濟新報文化事業股份有限公司以及中華安全科技與管理學會及臺灣網路防護協會共同主辦，以「《**管理系統驗證機構資通安全管理法驗證方案特定要求》資訊安全，網宇安全與隱私防護(cybersecurity and privacy protection)之標準化：根基於ISO/IEC 27001：2022(E)及ISO/IEC 27009：2020(E)**為標的及其在國家通資訊安全發展方案 (110年至113年)」中「**建立資通系統弱點之主動發掘、通報 及修補機制**」與「**完善政府網際服務網防禦深廣度**」之工作項目中的ISMS實作之議題規劃，希望對**資通安全管理法以及ISMS**的落實提供助益，誠摯的歡迎您參加。

- 時間：中華民國112年 06月07日（星期三）
- 地點：新北市板橋區民族路168號中華電信學院綜合大樓五樓G701禮堂
- 時程表

08:45~09:00 09:00~09:10	報到 致詞：台灣經濟新報文化事業股份有限公司 羅德興博士
09:10~10:25	**雲服務之容器安全與可信賴平台模組(Trusted Platform Module, 簡稱TPM及(Zero Trust Network, 簡稱ZTN)** **主講人：廣達電腦股份有限公司協理 宋振華博士**
10:25~10:35	休息

10:35~11:50	**資通安全管理法驗證方案特定要求之標準化:根基於ISO/IEC 27001:2022(E)及ISO/IEC 27009:2020(E)與自2014年起資通安全管理系統的過程取徑(Process approach)** 主講人:**台**灣經濟新報文化事業股份有限公司羅德興博士及樊國楨博士
12:00~13:30	午餐(供應便當)
13:30~14:45	**電信組織之資訊安全控制措施:根基於ISO/IEC 27002:2022(E)(ISO/IEC DIS 27011 · Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations:2022(E))** 主講人:臺北科技大學財金資訊系 魏銷志**教授**
14:45~14:55	休息
14:55~16:10	**個人資料管理系統要求事項:根基於ISO/IEC DIS 27701:2023(E)(Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines)** **主講人**:臺灣檢驗科技股份有限公**司 曾國維產品(PIMS)經理**

- 名額:現場50名(以報名先後排序)。
- 主辦單位保留因故變更議程之權利。
- 報名表:

資訊安全管理系統標準化系列討論會(112年06月07日)報名表

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。			
地址			
聯絡人		電話	
傳真		E-mail	
用　　餐	□葷　□素　(請擇一打勾)		

※注意事項:

- E-mail報名:fion.lw10@nycu.edu.tw, **網路報名**:http://www.tipa-service.org.tw/。
- 請於討論會前一週(05月31日)前完成報名手續, 以便行政作業之進行。
- 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, 請主動與方圓小姐[電話:0975-620512] 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:
  國家安全局

- 主辦單位:
  中華電信股份有限公司
  臺灣檢驗科技股份有限公司
  台灣經濟新報文化事業股份有限公司
  中華安全科技與管理學會
  臺灣網路防護協會