因應資通安全管理法公布-強化資訊安全管理系統(ISMS)

驗證機構之認證管理

驗證機構認證處/葉薇芬組長

資通安全管理法對 ISMS 資訊安全管理系統驗證之要求

我國於 107 年 5 月經立法院三讀通過「資通安全管理法」(以下簡稱資安法)，並於同年 6 月 6 日經總統公布，主要目的係積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。依據資安法第二條規定，資安法主管機關為行政院；第二十二條及第二十三條規定，施行細則及施行日期由主管機關定之。行政院於 107 年 11 月 21 日公告資安法與資安法六項子法(包括資通安全管理法施行細則、資通安全責任等級分級辦法、資通安全事件通報及應變辦法、特定非公務機關資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法，以及公務機關所屬人員資通安全事項獎懲辦法)於 108 年 1 月 1 日施行。

資安法納管對象包括公務機關(指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關)及非特定公務機關(指關鍵基礎設施提供者、公營事業及政府捐助之財團法人)，要求各機關訂定資安維護計畫，及訂定資安事件通報應變機制。行政院為提高政府機關(構)資訊安全管理水準，降低相關作業風險，自民國 90 年起即要求政府機關(構)推動資訊安全管理制度及驗證，90 年-93 年要求推動及實施推動資訊安全管理制度，94-97 年要求 A 級及 B 級責任等級於 96 年及 97 年通過 ISO/IEC 27001 驗證。隨著資安法及相關子法公告實施，依「資通安全責任等級分級辦法」，資通安全等級分為 A、B、C、 D、E 等五級(註[1])，屬於 A 級及 B 級機關者，初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維

註1 :責任等級之規定，請參考「資通安全責任等級分級辦法」第四條至第八條。

持其驗證有效性。有關第三方驗證，依「資通安全責任等級分級辦法」附表一、二、三、四備註第二點，「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。」，因此，資安法已明確揭示對 ISO/IEC 27001 資訊安全管理系統驗證之要求。

- **本會建立 ISMS 管理系統驗證之認證強化管理措施**

本會於 2003 年即開始提供 ISMS 資訊安全管理系統之認證服務，並分別於 2014 年及 2015 年簽署亞太認證合作組織(Asia Pacific Accreditation Cooperation, APAC)及國際認證聯盟(International Accreditation Forum, IAF) ISMS 多邊相互承認協議，依據 ISO/IEC 17021-1 及 ISO/IEC 27001 認證規範，對本會認證之驗證機構執行評鑑，以確保其持續符合本會認證要求。

本會因應資安法公告後，對國內資安防護機制及資通安全環境之重要性提升，於 2019 年 11 月 2 日召開「強化資訊安全管理系統(ISMS)驗證說明會」，特別邀請行政院資通安全處簡處長介紹資通安全法及子法規範，以及由本會說明針對資訊安全管理系統驗證認證評鑑重點及要求事項。資訊安全管理系統為具有高度技術且風險高之認證技術領域，因應國家法規要求及現今資訊安全管理系統之重要性，本會依據認證規範 ISO/IEC 17021-1 及 ISO/IEC 27006 評鑑，認證規範中之條款很明確要求驗證機構於執行稽核時應查核之項目，申請的組織亦必須符合 ISO/IEC 27001 之要求，藉由風險管理過程，保持資訊之機密性、完整性及可用性。驗證機構必須基於相關之技術專業為國內資訊安全把關，這些都是本會建立認證信賴之主要基礎，而每一個環節都攸關國內資通安全環境之健全及保障。

為強化 ISMS 管理系統驗證之認證管理，本會依據 ISO/IEC 17021-1 及 ISO/IEC 27006 條文要求，彙整評鑑查核重點(請參閱附表)，作為本會評鑑之關注方向：

	主題	ISO/IEC 17021-1:2015 ISO/IEC 27006:2015	查核重點
1.	公正性管理	ISO/IEC 17021-1:2015 第 5.2 節	• 輔導顧問公司與驗證之獨立性
2.	驗證範圍之認定	ISO/IEC 27006：2015 第 9.1.3.5 節	• 驗證範圍之適切性 • 涵蓋核心業務、功能(資通安全管理法施行細則第 7 條、主管機關要求)
3.	稽核人天之適足性	ISO/IEC 27006：2015 附錄 B, C	• 組織控制下的人數 • IT 複雜性及業務複雜度
4.	稽核報告充分詳細支持驗證決定	ISO/IEC 27006：2015 第 9.4.3.2 節	• 遵循的重要稽核軌跡及所用稽核方法 • 完成的問卷、查檢表、觀察紀錄、日誌或稽核員筆記可以構成稽核報告的一部分。若使用這些方法，上述文件應提供給驗證機構，作為支持驗證決定之證據。有關稽核期間被評估的樣本資訊應納入稽核報告或其他驗證文件中
5.	稽核證據	ISO/IEC 17021-1:2015 第 9.4.4.1 節	• 相關資訊經由適當的抽樣予以取得，並經查證而成為稽核證據
6.	稽核發現	ISO/IEC 17021-1:2015 第 9.4.5.2 節	• 不符合事項的稽核發現，則不應被記錄為改善的機會
7.	暫時終止、終止或減列驗證範圍	ISO/IEC 17021-1:2015 第 9.6.5 節	• 驗證客戶發生嚴重資安事件之處理 • 上述事件通報本會之機制(依本會管理系統認證方案服務手冊第 3.1.1 節)
8.	每次追查活動至少應審查項目	ISO/IEC 27006：2015 第 9.6.2.1.2 節	• 有關達成客戶資訊安全政策目的之 ISMS 有效性 • 定期評估及審查是否遵循相關資訊安全法律及法規的程序運作 • 控制項確定的變動，並導致 SoA 的變動 • 根據稽核方案所選控制項之實作與有效性
9.	重新驗證	ISO/IEC 27006：2015 第 9.6.3.1 節	• 重新驗證稽核之目的在於確認客戶管理系統整體的持續符合性與有效性，以及其驗證範圍的持續相關性與適切性 • 重新驗證稽核程序應與本國際標準中有關客戶 ISMS 初次的驗證稽核一致 • 允許進行矯正措施的時間，須與不符合事項的嚴重性及有關資訊安全風險相當

除了加強評鑑對認證規範之符合性，並採行幾項認證強化管理措施，包括:

(1) 辦理不定期監督評鑑。
(2) 評鑑小組增加技術專家隨隊。
(3) 增加總部評鑑人天。
(4) 增加見證評鑑場次。
(5) 與行政院資通處合作特定服務計畫。

前述認證強化管理措施，已於 2019 年 12 月展開試行，並列為後續檢討修正參考。

- **ISMS 資訊安全管理系統認證強化管理措施之重要性及效益**

實施此 ISO/IEC 27001 資訊安全管理系統驗證之組織(包含商業企業、政府機構及非營利組織)應於組織整體營運風險內建立、實施、運作、監視、審查、維持及改進已文件化之 ISMS 要求，並確保選擇適切及相稱之安全控制措施，故若能落實 ISMS 資訊安全管理系統制度之實施及達成驗證之有效性，鑑於資安法對國內公務機關及非特定公務機關之要求，可確保維護資訊資產並提供利害相關者信賴。

ISO/IEC 27001 資訊安全管理系統實施之落實，主要之責任在於推動及實施之機關本身，第三方驗證應基於公正、獨立、一致性之原則，依據驗證標準執行稽核，協助發現未滿足標準要求之缺失，以及管理系統運作之落實及維持。本會對於第三方驗證機構之認證強化措施，亦即要求其依認證規範，於稽核時明確界定驗證範圍、決定合理之稽核人天數、有效稽核證據之展現，以及不符合事項判定等執行內容及紀錄之強化，並要求法遵之關注事項。第三方驗證機構符合上述要求之驗證結果，將對國內建立資安防護機制及健全資通安全環境具有顯著效益及成果。

鑑於資安法對建構國家資通安全環境之重要性，本會於 ISMS 資訊安全管理系統認證服務，後續將針對資安法要求之法遵事項，建立資安法認證特定服務計畫，另訂定認證相關法遵要求，期共同為配合推動國家資安政策盡一份心力，擴大未來認驗證之效益及影響力，更提升社會大眾對認驗證之信心。