-「資通安全管理法驗證方案」認證服務介紹

驗證機構認證處/黃詠婕經理

- **行政院**「資通安全管理法」運用已與國際接軌之本會認證機制

「資通安全管理法」在政府積極推動「資安即國安」政策下，於 107 年 6 月 6 日經總統華總一義字第 10700060021 號令制定公布全文，並經 107 年 12 月 5 日行政院院臺護字第 1070217128 號令發布自 108 年 1 月 1 日施行，立法宗旨為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。

為提高政府機關(構)資訊安全管理水準，降低相關作業風險，行政院自 90 年起即開始推動資訊安全管理系統制度及驗證，並分別訂定資通安全管理法責任等級機關(A 級、B 級、C 級)之推動期程。規範對象包含公務機關、特定非公務機關，目的在提升資安防護、檢視內部資訊安全資源適足性及落實宣導，最後藉由認可機構對法遵要求的符合性進行把關。另「資通安全責任等級分級辦法」亦明定政府機關(構)資訊安全管理系統之導入及通過公正第三方驗證之相關規定，此辦法之第三方驗證即為運用本會認可機構之 ISO/IEC 27001 驗證結果。本會於 2015 年 10 月 21 日即簽署國際認證論壇(International Accreditation Forum, 簡稱 IAF) 資訊安全管理系統 (ISO/IEC 27001) 多邊相互承認協議 (Multilateral Recognition Arrangement，簡稱 MLA)，本會提供之認證服務已與國際接軌，亦即經本會認證之驗證機構驗證結果也可為國際間接受。

開放「資通安全管理法驗證方案」認證服務緣由與期程

本會早於 2003 年即提供資訊安全管理系統之自願性認證服務，為自實施以來，發生經驗證之政府機構仍發生重大的資安事件，為強化 ISMS 管理系統之運作，本會與行政院資通安全處於 108 年 12 月起，針對因應資通安全管理法施行，討論強化查核政府機關(構)資安維護計畫/實施情形、資安責任等級應辦事項、資通系統防護基準等法遵性驗證，經雙方充分評估與規劃，從強化認可機構的水準及稽核的品質，以提供健全的資通安全環境為目標，由本會基於 ISO/IEC 17021-1、ISO/IEC 27006 基礎下，增訂資通安全管理法驗證方案特定要求，自 2022 年 5 月 1 日受理開放「資通安全管理法驗證方案」認證服務。本項認證服務之規劃

與開放，有助於政府機關與產業界提升資安防護、組織強化，以及落實法制，具有重要的指標意義。

- **開放「資通安全管理法驗證方案」認證服務及認證規範介紹**

「資通安全管理法驗證方案」認證規範，除包含 ISO/IEC 17021-1 (符合性評鑑－機構提供管理系統稽核及驗證之要求－第 1 部：要求)及 ISO/IEC 27006:2015 / AMD 1:2020（資訊安全管理系統驗證機構認證規範）外，另訂定「資通安全管理法驗證方案特定要求」，包含驗證範圍、有效工作人員、稽核人天增加及計算、核心資通系統抽樣、場區抽樣、驗證機構人員能力要求、驗證報告等特定規範內容，確保驗證機構稽核作業遵循一致性驗證準則，改善現行因市場競爭驗證機構透過減少稽核人天，降低成本及收費，限縮驗證範圍，降低驗證成本，爭取客戶，以致造成作業品質等亂象；另外，也要求受稽核之政府機關(構)須確實將核心系統列入驗證範圍，來符合資訊安全的要求。取得本會此方案認證之驗證機構，除了基於相關之技術專業為國內資安防護把關，更重要的是受查核機關(構)符合資通安全管理法之法遵要求，這些都是本會建立認證信賴之基礎，且每一個環節都攸關國內資訊安全領域之健全及保障，亦突顯本項認證服務之迫切需求。