ISO/IEC 27006:2015 AMD 1:2020 資訊安全管理系統認證規範補充增修重點及 TAF 轉換規定

驗證機構認證處/黃詠婕

ISO/IEC 27006:2015AMD1:2020 補充增修內容

ISO/IEC 27006 資訊安全管理系統認證規範係針對資訊安全管理系統(ISMS)驗證機構明定要求並提供指引，其主要目的在於除 ISO/IEC 17021-1 要求外，支援 ISMS 驗證機構的認證作業。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，經本會認證之驗證機構執行資訊安全管理系統之驗證，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基礎，且每一個環節都攸關國內資通安全環境之健全及保障，亦突顯本項標準之重要性。

ISO/IEC 27006 於 2015 年改版後，2020 年微幅修訂部份條款內容，並於 2020 年 3 月 27 日發布 ISO/IEC 27006:2015 之第 1 次補充增修版本，共補充增修 6 項條文內容，分別是「7.2.1.1 d)遴選稽核員」、「8.2.1 ISMS 驗證文件」、「9.3.1.1 初次驗證稽核第一階段」、「B.2.1 組織控制下的工作人數」、「B.3.6 現場稽核時間」、「B.6 多場區的稽核時間」，並新增「7.2.1.1 有關遴選稽核員時須具備 ISO/IEC 27001 執行 ISMS 稽核的能力」，詳細內容可參照本會發佈之「資訊安全管理系統驗證機構認證規範(ISO/IEC 27006:2015 AMD1:2020)」規範文件。

本會對 ISO/IEC 27006:2015AMD1:2020 之轉換規定

國際認證論壇(International Accreditation Forum)於 2020 年 7 月 27 日發布「Transitional Arrangement for ISO/IEC 27006:2015 AMD 1:2020」決議事項，規範認證機構及驗證機構之轉換期程，驗證機構應於標準公告後 2 年(2022 年 3 月 31 日)，符合 ISO/IEC 27006:2015AMD 1:2020 標準之要求。

本會因應 IAF 訂定之轉換期程，發布認證作業通報 54，針對驗證機構轉換訂定相關做法和規定：

一、本會已認證及申請中之資訊安全管理系統(ISMS)驗證機構，應於 ISO/IEC 27006:2015 AMD1:2020 標準公告後 2 年(2022 年 3 月 31 日)，符合 ISO/IEC

27006:2015AMD 1:2020 標準之要求。

註：本次轉版並非標準版次之轉版，而係針對 ISO/IEC 27006:2015 於特定要求之變更以 AMD1:2020 版識別。

二、自 2021 年 1 月 1 日起，本會對已獲本會認證之資訊安全管理系統驗證機構之總部評鑑(延展評鑑、監督評鑑、增列評鑑)，將一併辦理 ISO/IEC 27006:2015 AMD 1:2020 轉換評鑑作業。完成前述總部評鑑及所列查核事項，並確認驗證機構之不符合報告改善完成，經審議通過者，即換發以 ISO/IEC 27006:2015 AMD 1:2020 為認證依據之認證證書。

本次因應 ISO/IEC 27006 認證規範之補充增修，除對稽核員資格及能力要求有變更外，針對多場區人天計算及有效人員數，亦做較清楚之詮釋。有關認證規範改版內容及 IAF 轉版之要求及期限，本會將定期於驗證機構座談會向本會申請中及已認可之驗證機構說明，且適時向驗證機構調查各項標準轉版之進度，以期認證機構、驗證機構及組織都能於轉版期程內完成相關轉版，符合市場需求，創造更高的認證價值。