

ISO/IEC 27001 : 2022

信息和數據安全管理系統 概況說明



您需要知道的

ISO/IEC 27001 是信息和數據安全管理系統 (ISMS) 的 ISO 標準。獲得 ISO/IEC 27001 認證的公司在信息和數據保護相關風險方面是合規的。

ISO 已宣布將 ISO/IEC 27001:2013 標準升級為 ISO/IEC 27001:2022。此次升級是由於 ISO/IEC 27002 中的更新，這標準支持和詳細說明了企業如何遵守 ISO/IEC 27001 附件 A 中的管控標準。

ISO 於 2022 年 2 月 15 日發布了新的 ISO/IEC 27002:2022 變更，ISO/IEC 27001 的附錄 A 將進行更新以與新的 ISO/IEC 27002 變更保持一致。新的 ISO/IEC 27001 標準於 10 月 25 日已發布。

ISO/IEC 27001 只進行了少量更改。但是，ISO/IEC 27001 的附件 A 管控將進行進一步的更改，以反映 ISO/IEC 27002:2022 標準中詳述之更新及修改。

ISO/IEC 27002:2022 的新名稱是信息安全、網絡安全及隱私保護—信息安全管控。

ISO/IEC 27001 有哪些新變化？

管控類別

更新的管控類別，已從 114 個減少到 93 個管控，其分佈在四個類別中：組織、人員、物理和技術。

- 58 個管控在更新後保持不變
- 24 個管控已合併
- 添加了 11 個管控

雲端安全現在是該標準涵蓋的一個新領域，而 ISO/IEC 27001:2013 之前並未涵蓋。

ISO/IEC 27002:2022 現在提供了更透明的管控結構，可以在整個組織中應用。這些管控現在就網絡安全及隱私保護方面之人為因素，提供了更多技術建議。

屬性

現在每個管控皆引入了屬性。ISO/IEC 27001 中的屬性允許組織創建不同的見解，這些見解是從不同角度看到的不同的管控分類；換句話說，它將使組織能夠將管控導向正確的受眾。

組織可以創建自己的屬性，下面列出的每個屬性都帶有一系列對應的屬性值。

- 管控類型
- 信息安全屬性
- 網絡安全概念
- 運營能力
- 安全領域

已經有 ISO/IEC 27001?
您的組織將有 3 年時間過渡到新版本的標準。

IMSM 參與標準的升級、過渡和轉移超過 25 年，並擁有專業、固定費用和增值的過渡計劃 - 我們建議您儘早與我們聯繫以探索合適的選項，確保您能執行新版本的標準。



聯繫我們