

bsi.

● ISO/IEC 27001 轉版指南

大幅提升ISMS資訊安全管理系統的有效性

隨著數位化改變了全球的數位格局，許多商業實務如遠端工作、自攜電子設備 (Bring Your Own Device) 和工業 5.0 等，變得更加依賴雲端和數位。為協助企業更順利地因應這樣的變化，「ISO/IEC 27001 資訊安全管理」和「ISO/IEC 27002 資訊安全控制措施」標準正式推出了更新改版，提供更完善且符合資訊安全風險環境的控制措施，確保與您組織的整體環境保持一致。



步驟 1 - 瞭解變更項目

選擇新版 ISO/IEC 27001:2022 和 ISO/IEC 27002:2022 標準，我們提供了相關的教育訓練課程與免費資源，能協助您和團隊成員瞭解變更的項目，順利完成轉版之旅。



技能更新

參加 BSI ISO 27001 [最新教育訓練課程](#)，讓您和團隊都能為轉版做好準備。

步驟 2 - 確認對組織的影響

運用您於 BSI 教育訓練課程所學的新知輔以 ISO/IEC 27002，進行組織風險評估和新版 ISO/IEC 27001 的差異分析，確保與您組織的背景和目標一致。



更新就緒

到這個階段，您可以準備開始更新 ISO/IEC 27001 證書了。

步驟 3 - 採用變更項目

請檢視納入或排除必要控制措施的證據和理由，並據此更新您的適用性聲明 (SOA)。務必根據您的風險處理計畫和新的控制措施來建置合適的改變。藉由內部稽核來確認這些變更項目是否被有效實施，此階段將協助您減少可能的失誤。一切備妥後，與我們聯絡安排進一步稽核。



看見優勢

即使在轉版流程的初期，您也能透過差異分析瞭解公司當前的營運流程及相關風險，進而看到採用這些變更項目後所帶來的好處與優勢。

步驟 4 - 轉換您的證書

聯絡您的 BSI 企業服務部代表，預約安排轉版稽核服務。您的客戶經理將會進一步確認您所選擇新控制措施的執行狀態，及是否與資訊安全管理系統 (ISMS) 一致，以協助您順利轉換到新版 ISO/IEC 27001:2022。於此同時，您也能從稽核報告，瞭解稽核員的回饋建議，並做後續改善動作。



大功告成！

恭喜您完成所有流程，取得新版 ISO/IEC 27001:2022 證書。

保持合規並持續優化

持續改善您的管理流程，並強化組織內部的資訊韌性。