ISO/IEC 27001:2022 轉版常見問題

Learn from the experts

1. 2022 標準已發布了嗎？

是的，ISO 27001:2022 已於 2022 年 10 月 25 日發布。

2. 新版標準有哪些關鍵變更？

附錄 A 是本次修訂的關鍵更動，反映了 ISO/IEC 27002:2022 的變化。這些更動為：

- **結構已合併為 4 大關鍵領域：** 組織、人員、實體和技術，而不是上一版中的 14 個。
- **列出的控制措施從 114 項減少到 93 項。**

本文中的調整（如）：

- 將文中的「國際標準」改為「文件」。
- 部分英文重新調整，以利於翻譯。

此外，為符合新的 ISO 調和結構而做的更動：

- 編號結構微調。
- 要求定義實施資訊安全管理系統（ISMS）所需的流程以及它們之間的相互作用。
- 明確要求在組織內溝通與資訊安全有關的組織角色。
- 新增條款 6.3 一變更的規劃。
- 在條款 7.4 中新增要求確保組織確認如何進行溝通。
- 新增要求為「作業流程」和「實施流程控制措施」建立標準。

3. 是否必須採用 ISO/IEC 27002:2022 才能過渡到 ISO/IEC 27001:2022？

雖然沒有強制規定，但新版的 ISO/IEC 27002:2022 現在涵蓋了許多新增的分組、屬性和描述等項目，讓 ISO/IEC 27001:2022 控制措施能更容易地被有效實施，且更容易與網路安全架構和其他風險管理方法保持一致。

4. 我們正在採用 ISO/IEC 27001:2013，此版本是否還能做為 ISMS 有效驗證？

若您申請以 ISO/IEC 27001:2013 進行驗證，須在 2025 年 10 月 31 日前完成轉換。然而，依據 2023 年 3 月中旬之最新公告及要求，若想以舊版驗 2013，就須注意截止日由原先 2023 年 10 月底調整改為 2024 年 4 月底，而原 2023 年 11 月 1 日開始需使用新版做驗證的時程也調整改至 2024 年 5 月 1 日，故在 2024 年 5 月 1 日之後，新申請之驗證不可再使用 ISO/IEC 27001:2013 版本稽核，所以建議您在此階段申請驗證，最好選擇以新版進行驗證較佳。

5. 若 2025 年 10 月前為轉換截止期限，為何我們現在就要採取行動？

因應數位化帶來工作方式和相關威脅的轉變，新版的 ISO/IEC 27001:2022 標準提供了更完善的控制措施，不但符合資訊安全風險環境，更重要的是與您組織的整體環境一致。因此，盡早準備新版過渡是非常重要的：

- 確保您的資訊安全系統能有效因應目前的數位環境和相關風險。
- 透過採用更彈性的控制架構與全球網路安架構保持一致，從而獲取最大效益。
- 將管理系統更新與調合結構一致，以提高管理系統的效率。

6、請問何時會有相關教育課程訊息釋出？

為協助您和團隊成員瞭解變更項目順利完成轉版之旅，BSI 提供了相關的教育訓練課程。最新 ISO/IEC 27001:2022 教育訓練課程請參考 BSI 教育訓練課程網頁。歡迎訂閱 BSI 免費電子報，即時獲得轉版最新動態與開課資訊！

名稱	預計天數
基礎課程	2 天
內部稽核員課程	2 天
風險管理課程	2 天
建置課程	3 天
CQI & IRCA 主導稽核員課程	5 天
主導稽核員轉版課程	2 天
CQI & IRCA 稽核員轉換課程	3 天

7. 轉版時程預計多長？

轉版過渡期為期三年，從 2022 年 11 月 1 日到 2025 年 10 月 31 日。您務必要完成 貴公司資訊安全管理系統的轉版作業，同時需在此期間內的後續審查時，接受 BSI 採用新標準對您的系統稽核並取得 ISO/IEC 27001:2022 的證書，否則在截止日 2025 年 10 月 31 日後，舊版證書將會失效。

8. 變更會對我們的資訊安全管理系統產生什麼影響？

關鍵影響將是需要重新審視您的風險評估和適用性聲明，以確保適當有效地應用修訂後的控制措施，讓您的資訊安全管理系統（ISMS）更能因應數位轉型帶來的相關風險。

9.我們應該如何轉版和更新證書？

您可選擇在 ISO/IEC 27001:2022 公佈後 3 年內的任何一次定期性後續稽核進行轉版稽核。轉版稽核將能協助評估這些變更是否有效被實施。此外，您還需全盤了解這些變更項目及其對組織的影響，以順利完成轉版。BSI 建議您詳讀標準相關資訊、參加教育訓練課程，並安排轉版稽核服務，以確保您的資訊安全管理系統（ISMS）能有效保護您企業的數位資產，並順利完成新版轉換。