互動式PDF

ISO/IEC 27001:2022 有哪些變更？

新版 ISO/IEC 27001 已於 2022 年 10 月發布，建議您即早更新組織的資訊安全管理系統（ISMS），以有效因應數位環境變化所帶來的挑戰。

這份互動文件能夠提供您關於變更的摘要。如欲深入瞭解詳情，歡迎報名BSI教育訓練課程。

編緝性修改

新增的要求事項

四大新增之資訊安全控制措施參考指引

條款5
組織控制措施

條款6
人員控制措施

條款7
實體控制措施

條款8
技術控制措施

修訂後附錄A的資訊安全控制措施

控制措施從114項減少到93項

24
合併

58
修訂

11
新增

新增五項有助分類和風險處理的控制措施屬性

控制措施型式

資訊安全性質

網宇(路)安全概念

運作能力

安全領域

儘管新版標準過渡期為三年，為確保您的資訊安全管理系統（ISMS）能因應當前的網路和資訊安全環境，建議您現在就開始採取行動！

歡迎與我們的企業服務團隊聯絡，進一步了解如何順利完成新版轉換

bsigroup.com.tw | +886 2 2656 0333 | infotaiwan@bsigroup.com

編緝性修改

- 完全符合新的ISO調和結構 (Harmonized Structure)

  ISO管理系統標準的基本原則是它們能夠共同協作。因此，新版的ISO/IEC 27001也能與其他標準共同使用。透過強調流程導向，可以使參與管理系統的利害關係人更清楚地了解流程的進行。同時，有助於在管理系統實施的過程中實現簡化和一致性。

- 重新編排部分英文內容以利翻譯
- 將子編號的結構重新編排，以便與調和方法保持一致
- 不再提及控制目標，因為它們已自附錄 A 或 ISO/IEC 27002 移除
- 新條款 6.3 – 變更之規劃

新增的要求事項

- 定義實施和維護資訊安全管理系統（ISMS）所需過程及其互動
- 在組織內部傳達與資訊安全相關的組織角色
- 監視資訊安全目標
- 根據條款 7.4，確保組織確認如何溝通的新要求
- 建立過程之準則及依準則實作過程之控制措施
- 確保與資訊安全管理系統相關外部所提供之過程、產品或服務受控制

四大新增之資訊安全控制措施參考指引

條款5

組織控制措施

這些控制項目擁有廣泛的範疇，包括組織層面的管理政策或供應鏈中的資訊安全。

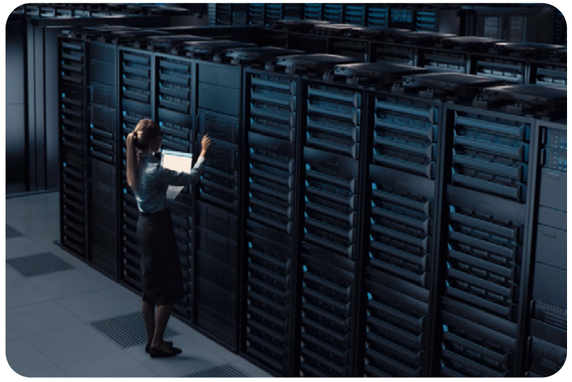
- 37 項控制措施
- 34 項既有
- 3 項新增

條款6

人員控制措施

這些控制項目牽涉到與人員有關的事項，包括教育訓練、聘用條款及條件等各方面議題。

- 8 項控制措施
- 皆為既有控制措施



條款7

實體控制措施

這些控制項目牽涉到對實體區域或設備的保護，包括實體進入及設備汰除或重新使用之保全等控制措施。

- 14 項控制措施
- 13 項既有
- 1 項新增

條款8

技術控制措施

這些控制措施與技術相關。例如，安全鑑別技術與組態管理。

- 34 項控制措施
- 27 項既有
- 7 項新增

修訂後附錄A的資訊安全控制措施 - 從114項減少到93項

24 合併

為什麼有些控制措施被合併？

在新版標準中，24項先前無法分割或密切相關的控制措施被合併，這是由於ISO/IEC 27001採用了更加強調流程導向及調和方法所致。

例如，在先前的標準中，有三個獨立的控制措施與存取和存取控制相關，現在則合併為一個控制措施，要求對發展、實施和維護存取控制進行完整定義的流程。

為什麼這很重要？

這些合併導致特定的細節並未在新合併的控制措施中直接列出，但可以通過對流程、相互關係和流程標準的清晰定義來理解或推斷這些細節。這意味著您必須首先檢視標準的主要部分、您組織的全景、其規劃和運作。

只有當您確定了您的流程和互動之後，才應該開始處理新合併的控制措施。

58 修訂

有哪些預期的改變？

這58項控制措施已經經過修訂和更新，以確保它們在當前的商業環境中適用，且可以應對當前的各種威脅和風險。隨著遠端工作成為風險管理的一個重要部分，相應的控制措施已經被重新命名和更新。

我需要做什麼？

儘管這些控制措施的修訂程度不同，但都經過審查，並且有些已進行了大幅更新。您必須檢查更新的指南，以確保完全掌握修訂後的控制措施，以應對您業務目前的運作方式和所面臨的威脅。

11 新增

有哪些新增的控制措施？

在過去十年中，出現了新的風險領域，如雲端運算和隱私要求，促使人們制定新的控制措施來應對這些風險。還有一些專門針對變得更加重要的流程進行了正式規範，如對IT部門和組織本身的威脅分析和營運持續。以下是新的控制措施：

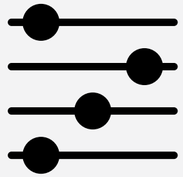
- 組織控制措施
  - 威脅情資
  - 使用雲端服務之資訊安全
  - 營運持續之ICT備妥性
- 實體控制措施
  - 實體安全監視
- 技術控制措施
  - 組態管理
  - 資訊刪除
  - 資料遮蔽
  - 資料洩露預防
  - 監視活動
  - 網頁過濾
  - 安全程式設計

最佳實務是什麼？

ISO/IEC 27002的最新版本提供了有關每個新控制措施的專屬資訊，包括最佳實務做法以及如何確保您保持合規性。

新增五項有助分類和風險處理的控制措施屬性

這些控制措施屬性如何協助分類和風險處理？



控制措施型式

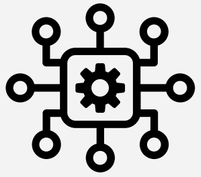
控制的三個基本類型包括預防性（在漏洞首次發生前阻止它）、偵測性（在發生漏洞時發出警報）和矯正性（在漏洞發生後進行補救）。了解您的系統如何平衡這三個方面有助於了解您對風險管理的整體方法。

資訊安全性質

資訊安全的三大原則是機密性、完整性和可用性。新版標準中的每個控制措施屬性現在都有標籤，以顯示它是否支援其中一個或多個原則。這使得評估您的控制實施變得更加容易，以確保它覆蓋業務所需的機密性、完整性和可用性的適當平衡。

網宇(路)安全概念

這個屬性讓您可以根據控制措施來將其分類，確認是否有助於建立一個除保護系統之外強大安全的系統。這包括識別現有和新興的威脅、保護您的資產、偵測可疑活動，並對入侵或攻擊進行回應和回復。



運作能力

組織可以採用多種運作能力來保護其資訊資產。透過對這些屬性進行篩選，您可以了解需要哪些能力來支持您所需的控制措施組合，以應對組織風險。

安全領域

安全領域還可以分為治理和生態系統、保護、防禦和韌性。根據這些屬性篩選您的控制措施，可以確保您的措施在這些領域中得到適當的平衡，以符合您組織的風險要求。