ISO 27001改版簡介

國家資通安全研究院

簡報大綱

- 前言
- 標準名稱修改
- ISO 27001改版重點
- ISO 27002改版重點
- 結論與建議

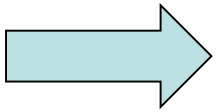
前言

- ISO/IEC 27002:2022於2022年2月發布，ISO/IEC 27001:2022於2022年10月發布
- CNS 27001:2023、CNS 27002:2023於2023年1月一起發布
- 2022版相較於前次2013版，在資訊安全基礎上納入網宇安全及隱私保護概念

標準名稱修改

ISO/IEC 27001:2013
Information technology - Security techniques - Information security management systems – Requirements

資訊技術 - 安全技術 - 資訊安全管理系統 - 要求事項

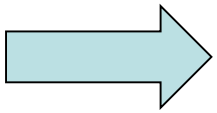


ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection - Information security management systems – Requirements

資訊安全、網宇安全及隱私保護 - 資訊安全管理系統 - 要求事項

ISO/IEC 27002:2013
Information technology - Security techniques - Code of practice for information security controls

資訊技術 - 安全技術 - 資訊安全控制措施之作業規範



ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection - Information security controls

資訊安全、網宇安全及隱私保護 - 資訊安全控制措施

ISO 27001改版重點

- 本文除部分條款有額外要求新增、用語調整、備考(Note)說明調整、架構變更及條款編號互換外，僅新增全新子條款1項
- 附錄 A 由原先14類整併為組織、人員、實體及技術等4大主題，控制措施也由114項調整為93項，同時於ISO 27002提供屬性標籤，讓控制措施更容易使用(附錄A直接取自ISO 27002)

新增條款

6.3 變更之規劃 (Planning of changes)

當組織決定需要對資訊安全管理系統變更時，應以規劃之方式執行變更。

新增要求/用語調整/架構變更(1/7)

4.2 瞭解關注方之需要及期望 (Understanding the needs and expectations of interested parties)

組織應決定：

a) 與資訊安全管理系統有關之關注各方；

b) 此等關注方之相關**要求**事項；

c) 此等要求事項中之哪些要求事項，將透過資訊安全管理系統因應。

備註：關注方之要求事項**可能**包括法律及法規要求及契約義務

新增要求/用語調整/架構變更(2/7)

4.4 資訊安全管理系統

(Information security management system)

組織應根據本**文件**之要求事項，建立、實作、維持及持續改善資訊安全管理系統，**包括所需過程及其互動**。

新增要求/用語調整/架構變更(3/7)

6.2 資訊安全目標及達成之規劃 (Information security objectives and planning to achieve them)

組織應在各相關部門及層級建立資訊安全目標。

資訊安全目標應滿足下列事項：

a)與資訊安全政策一致。

b)可測量（若可行）。

c)考量適用的資訊安全要求事項，以及風險評鑑及風險處理之結果。

d)受監視。

e)被傳達。

f)於適切時，更新之。

g) 以文件化資訊提供。

新增要求/用語調整/架構變更(4/7)

7.4 溝通或傳達(Communication)

組織應決定，相關於資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項：

a)溝通或傳達事項。

b)溝通或傳達時間。

c)溝通或傳達對象。

d)溝通或傳達方式。

備註：刪除 d)溝通或傳達人員及e)進行有效溝通或傳達所採用過程

新增要求/用語調整/架構變更(5/7)

8.1運作之規劃及控制(Operational Planning and control)

組織應規劃、實作及控制符合要求事項所需之過程，並藉由下列方式，實作第6 節所決定的行動：

- **建立過程之準則(criteria)。**
- **依準則實作過程之控制措施。**

應保存應提供文件化資訊，其程度須具足以達成其過程已依規劃執行之信心。

組織應控制所規劃之變更，並審查非預期變更的後果，必要時採取行動以減輕任何負面效果。

組織應確保**相關於資訊安全管理系統之外部提供的過程、產品或服務**受控制。

新增要求/用語調整/架構變更(6/7)

9.1 監督、量測、分析及評估

(Monitoring, measurement, analysis and evaluation)

組織應決定下列事項：

a) 需要監督與量測之事項，包括資訊安全過程及控制措施。

b) 監督、量測、分析及評估之適用方法，以確保有效的結果。**所選擇之方法宜產生適於比較及可重製視為有效之結果。**

c) 應執行監督與量測之時間。

d) 應執行監督與量測之人員。

e) 監督及量測結果應分析及評估之時間。

f) 應執行分析及評估上述結果之人員。

應提供文件化資訊，作為結果之證據。

組織應評估資訊安全績效及資訊安全管理系統之有效性。

架構變更/用語調整/新增要求(7/7)

9.2 內部稽核(Internal audit)

9.2.1 一般要求(General)

9.2.2 內部稽核計畫(**Internal audit programme**)

(用語微調)

9.3管理審查(Management review)

9.3.1 一般要求(General)

9.3.2 管理審查輸入(**Management review input**)

管理審查應包括對下列事項之考量。

a)過往管理審查之議案的處理狀態。

b)與資訊安全管理系統有關之外部及內部議題的變更。

c)與資訊安全管理系統相關關注方之需要及期望的變更。

9.3.3 管理審查結果(**Management review result**)

(用語微調)

條款編號互換

10 改善(Improvement)

- ISO 27001:2013
  - 10.1 不符合事項及矯正措施
  - 10.2 持續改善

- ISO 27001:2022
  - 10.1 持續改善
  - 10.2 不符合事項及矯正措施

ISO 27002改版重點

- 將控制措施由舊版14個控制領域整合成4大主題(theme)
  - 組織控制(Organization Controls)37項(34項既有，3項新增)
  - 人員控制(People Controls)8項(皆為既有措施)
  - 實體控制(Physical Controls)14項控制(13項既有，1項新增)
  - 技術控制(Technological Controls)34項控制(27項既有，7項新增)
- 由舊版114項控制措施調整為93項控制措施
  - 全新之控制措施11項
  - 更新之控制措施58項(淘汰過時技術，反映最新的最佳實務)
  - 合併之控制措施24項(將不可分割或密切相關的既有控制措施加以合併)
- 加入5項可供選擇與搜尋的屬性
- 「目的(Purpose)」取代「控制目標(Control Objectives)」

全新控制措施(1/11)

A.5.7 威脅情資(Threat intelligence)

控制措施

應蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資

目的

提供對組織威脅環境之認知，以便採取適切的減緩措施

實務指引

- 蒐集(例如CERT、ISAC 、 CVE) 並分析有關既有或新出現威脅之資訊，以防止或降低威脅對組織造成傷害與衝擊(例如作為防火牆、IDS/IPS之輸入)
- 威脅情資分為策略型(如攻擊型式)、戰術型(如攻擊工具) 、運作型(如攻擊細節)
- 落實資通安全管理法-資通安全情資分享辦法
- 將威脅情資納入組織的風險管理過程

全新控制措施(2/11)

A.5.23 使用雲端服務之資訊安全(Information security for use of cloud services)

控制措施

應依組織之資訊安全要求事項，建立獲取、使用、管理及退出雲端服務的過程

目的

規定並管理使用雲端服務之資訊安全性

實務指引

- 組織應進行雲端服務風險評鑑，明確識別可接受之剩餘風險
- 針對雲端服務供應商與組織間的協議，應包括關於保護組織資料及服務可用性之條款
- 訂定雲端服務資安要求，以及雲端服務提供者與組織間雙方責任
- 訂定雲端服務作業程序(安全管控、定期查核、變更管理、安全退出)

全新控制措施(3/11)

A.5.30 營運持續之ICT備妥性(ICT readiness for business continuity)

控制措施

應依營運持續目標及ICT持續之要求事項，規劃、實作、維護及測試ICT備妥性

目的

確保於中斷期間，組織之資訊及其他相關聯資產的可用性

實務指引

- 進行營運衝擊分析(BIA)時，將ICT回復服務所需的RTO及步驟納入考量，並訂定ICT持續計畫 (包含詳細述明組織如何規劃管理ICT服務中斷之回應及復原程序)
- ICT持續計畫需透過演練及測試，並定期評估
- 資通安全責任等級分級辦法-業務持續運作演練

全新控制措施(4/11)

A.7.4 實體安全監視(Physical security monitoring)

控制措施

應持續監視場所，防止未經授權之實體進出

目的

偵測並阻止未經授權之實體進出

實務指引

- 安裝視訊監視系統(如閉路電視)，以查看並記錄組織場所內外敏感區域之進出
- 安裝並定期測試(尤其組件由電池供電時)接觸、聲音或移動之偵測器以觸發入侵者警報，警報器需涵蓋對外門窗
- 所有監視及記錄機制之使用，皆應考慮當地法律及法規，特別是關於人員監視及錄製視訊之留存期限

全新控制措施(5/11)

A.8.9 組態管理(Configuration management)

控制措施

應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)

目的

確保硬體、軟體、服務及網絡於所要求安全設定下正常運行，且組態未遭未經授權或不正確變更而更改

實務指引

- 應備妥角色、責任及程序(如資訊資產管理程序書或組態管理程序書)，以確保所有組態建立與變更皆符合要求
- 使用公開可取得之安全組態標準模板(如GCB、廠商及獨立安全組織提供之組態最佳化模板)
- 可藉由自動化或人工方式比對分析組態是否偏差，並採取矯正措施
- 組態設定模板及標的可能係機密資訊，需妥善防護

全新控制措施(6/11)

A.8.10 資訊刪除(Information deletion)

控制措施

當於資訊系統、裝置或所有其他儲存媒體中之資訊不再屬必要時，應刪除之

目的

防止敏感性資訊之非必要暴露，並遵循資訊刪除的法律、法令、法規及契約要求

實務指引

- 依營運要求，並考量相關法律法規，選擇刪除之方法(如銷毀、電子覆寫、消磁、恢復出廠設定等)
- 資訊刪除的證據需留存 (含自主與委外)
- 第三方代為儲存組織資訊(如雲端服務)，應考量將資訊刪除之要求納入協議

全新控制措施(7/11)

A.8.11 資料遮蔽(Data masking)

控制措施

應使用資料遮蔽，依組織關於存取控制之主題特定政策及其他相關的主題特定政策，以及營運要求事項，並將適用法令納入考量

目的

限制內含PII之敏感性資料的暴露，並遵循法律、法令、法規及契約的要求

實務指引

- 去識別化分為匿名化(無法辨識為PII)與假名化(不借助額外資訊情況下無法識別出個人資訊主體)。若採用假名化，須將能比對出個人資訊主體的額外資訊分開保存並受保護。
- 資料遮蔽技術包含加密、清空或刪除字元、變更數字或日期、替換、以雜湊值替換原值(可合併加鹽)
- 不對使用者授予所有資料之存取權限(設計查詢及遮罩，可僅向使用者顯示所要求的最少資料)

全新控制措施(8/11)

A.8.12 資料洩露預防(Data leakage prevention)

控制措施

應將資料洩露預防措施，套用至處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置

目的

偵測並防止個人或系統未經授權揭露及擷取資訊

實務指引

- 識別資訊並分類分級以防止洩露（如個人資訊、日誌資訊）
- 監視資料洩漏管道（如電子郵件、檔案傳送、行動裝置及可攜式儲存裝置）
- 採取措施防止資訊洩露（如阻止將機敏資訊儲存至可攜式設備）
- 可使用資料外洩預防工具，協助管理識別、監視及措施防止

全新控制措施(9/11)

A.8.16 監視活動(Monitoring services)

控制措施

應監視網路、系統及應用之異常行為，並採取適切措施，以評估潛在資訊安全事故

目的

偵測異常行為及潛在資訊安全事故

實務指引

- 應建立正常行為之基準(存取時間/位置/ 頻率)，並依此基準監視異常
- 使用監視工具進行持續監視，並善用威脅情資、機器學習/AI 及黑白名單
- 監視活動應依預先定義之門檻值產生警示(如經由管理控制台、電子郵件訊息或即時通訊系統)

全新控制措施(10/11)

A.8.23 網頁過濾(Web filtering)

控制措施

應管理對外部網站之存取，以降低暴露於惡意內容

目的

保護系統免受惡意軟體之危害，並防止存取未經授權的網頁資源

實務指引

- 組織應識別員工宜或不宜存取之網站型式，並封鎖存取惡意網站(如具資訊上傳功能之網站、已知或可疑之惡意網站、C&C伺服器、由威脅情資中獲取之惡意網站及分享非法內容之網站)
- 建立安全及適切使用線上資源(包含網站存取)之規則，並提供教育訓練
- 存取規則部署於網路控制工具(如防火牆)，並定期檢視與更新

全新控制措施(11/11)

A.8.28 安全程式設計(Secure coding)

控制措施

軟體開發應施行安全程式設計原則

目的

確保軟體係安全的撰寫，從而降低軟體中潛在資訊安全脆弱性之數量

實務指引

- 組織應建立流程，針對程式開發前/中/後三階段提出最低安全準則
  - 開發前規劃事項，例如使用更新之開發工具、設定開發工具之組態
  - 開發期間考量事項，例如禁止使用不安全之設計技術(如硬編碼通行碼)
  - 審查及維護，例如安全包裝與部署、原始碼保護、記錄錯誤並定期審查Log
- 應涵蓋第三方及開放原始碼的軟體
- 應監視真實世界之威脅及關於軟體脆弱性的最新建議與資訊

控制措施屬性

- 每項控制措施前加入5項控制屬性(Attributes)標籤，以 # 標註，其主軸精神使組織利用標籤化來查找對應之控制措施
- 控制措施屬性與其屬性值
  - **控制措施型式**：預防性、偵測性、矯正性
  - **資訊安全性質**：機密性、完整性、可用性
  - **網宇安全概念**：識別、保護、偵測、回應、復原
  - **運作能力**：治理、資產管理、資訊保護、人力資源安全、實體安全、系統與網路安全、應用程式安全、安全組態、識別與存取管理、威脅與脆弱性管理、持續性、供應商關係安全、法律與遵循性、資訊安全事件管理、資訊安全保障
  - **安全領域**：治理及生態系統、保護、防禦、韌性

治理及生態系統 包括資訊系統安全治理及風險管理、生態系統網宇安全管理

保護 包括IT安全架構、IT安全管理、身分識別與存取管理、IT安全維護、實體及環境安全

防禦 包括偵測、電腦安全事故管理　　韌性 包括運作之持續性、危機管理

結論與建議

- 新版ISO 27001條款變動不大，多屬於增強舊版精準度及調和整體架構
- 已導入ISO27001之組織，需重新檢視相關程序書，並更新適用性聲明
- 因應ISO 27001改版，以此標準為基礎擴展之其他標準，現階段也正檢討中，後續需持續關注相關ISO標準之改版情形

報告完畢
敬請指教