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

勘誤表(1)　　勘誤日期：112 年 6 月 1 日

頁次	位置	原文	更正
9	8.1 第五行	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。	應保存並提供文件化資訊，其程度須具足以達成其過程已依規劃執行之信心。

ICS 35.030

中華民國國家標準

C N S

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

Information security, cybersecurity and privacy protection − Information security management systems − Requirements

CNS 27001:2023
X6049

中華民國 95 年 6 月 16 日制定公布
Date of Promulgation:2006-06-16

中華民國 112 年 1 月 30 日修訂公布
Date of Amendment:2023-01-30

目錄

(共 24 頁)

前言

本標準係依據 2022 年發行之第 3 版 ISO/IEC 27001，不變更技術內容，修訂成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。CNS 27001:2014 已經修訂並由本標準取代。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

0.1 一般

本標準之制定旨在提供用以建立、實作、維持及持續改善資訊安全管理系統(information security management system, ISMS)之要求事項。採用資訊安全管理系統為組織之策略性決策(strategic decision)。組織之資訊安全管理系統的建立及實作受組織之需要及目標、安全要求事項、所使用之組織過程與組織的規模及結構所影響。預期所有此等影響因素將隨時間改變。

資訊安全管理系統藉由應用風險管理過程，保持資訊之機密性、完整性及可用性，並就已適切管理風險，賦予關注方信心。

資訊安全管理系統為組織各項過程及整體管理結構之一部分，並與之整合係屬重要，且於過程、資訊系統及控制措施之設計中，考量資訊安全亦屬重要。預期資訊安全管理系統之實作，將依組織需要調整。

本標準可由內部及外部各方使用，以評鑑組織符合組織自身資訊安全要求事項之能力。

本標準各項要求事項呈現之順序，並不反映其重要性或隱含其實作順序。列舉條目編號僅供參引之用。

CNS 27000 引用資訊安全管理系統系列標準(包括 CNS 27003[2]、CNS 27004[3]及 CNS 27005[4])，描述資訊安全管理系統之概觀及詞彙，以及相關用語及定義。

0.2 與其他管理系統標準之相容性

本標準適用 ISO/IEC Directives, Part 1, Consolidated ISO Supplement 之附錄 SL 所定義的高階結構，相同節次標題、相同文字、共同用語及核心定義，因此得以與其他已採用該附錄之管理系統標準維持相容性。

此定義於該附錄之共同作法，對選擇運作單一管理系統，以滿足 2 或多個管理系統標準要求事項的組織係屬有用。

1. 適用範圍

本標準規定於組織全景內，建立、實作、維持及持續改善資訊安全管理系統之要求事項。本標準亦包括依組織需要而裁適之資訊安全風險評鑑及處理的要求事項。本標準敘述之要求事項係屬通用，旨在適用於所有組織，不論其型式、規模或性質。當組織宣稱符合本標準時，不得排除本標準第 4 節至第 10 節所規定之任何要求事項。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括補充增修)。

CNS 27000 資訊技術－安全技術－資訊安全管理系統－概觀及詞彙

3. 用語及定義

CNS 27000 所規定之用語及定義適用於本標準。

4. 組織全景

4.1 瞭解組織及其全景

組織應決定與其目的有關且影響達成其資訊安全管理系統預期成果能力之外部及內部議題。

備考：決定此等議題，係指建立於 CNS 31000[5]之 5.4.1 中所考量的組織外部及內部全景。

4.2 瞭解關注方之需要及期望

組織應決定下列事項：

(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。

備考：關注方之要求事項可能包括法律及法規要求事項，以及契約義務。

4.3 決定資訊安全管理系統之範圍

組織應決定資訊安全管理系統之邊界及適用性，以建立其範圍。

於決定此範圍時，組織應考量下列事項：

(a) 4.1 中所提及之外部及內部議題。

(b) 4.2 中所提及之要求事項。

(c) 組織執行之活動與其他組織執行的活動間之介面及相依性。

範圍應以文件化資訊提供。

4.4 資訊安全管理系統

組織應依本標準之要求事項，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。

5. 領導作為

5.1 領導及承諾

最高管理階層應藉由下列事項，展現對資訊安全管理系統之領導及承諾：

(a) 確保已建立資訊安全政策及資訊安全目標，並與組織之策略方向相容。

(b) 確保資訊安全管理系統要求事項整合入組織之各項過程。

(c) 確保資訊安全管理系統所需之資源可取得。

(d) 傳達有效之資訊安全管理的重要性，以及符合資訊安全管理系統要求事項之重要性。

(e) 確保資訊安全管理系統達成其預期成果。

(f) 指導及支援人員，以促進資訊安全管理系統之有效性。

(g) 推動持續改善。及

(h) 當適用其他相關管理角色之責任範圍時，加以支持以展現其領導權。

備考： 本標準所提及之〝營運〞，能廣義詮釋為對組織存在目的具核心意義之該等活動。

5.2 政策

最高管理階層應建立包含下列事項之資訊安全政策：

(a) 適合於組織之目的。

(b) 包括資訊安全目標(參照 6.2)或提供設定資訊安全目標之框架。

(c) 包括對滿足相關於資訊安全之適用要求事項的承諾。

(d) 包括對持續改善資訊安全管理系統之承諾。

資訊安全政策應符合下列項目：

(e) 以文件化資訊提供。

(f) 於組織內傳達。

(g) 適切時，提供予關注方。

5.3 組織角色、責任及權限

最高管理階層應確保資訊安全相關角色之責任及權限已於組織內指派並傳達。

最高管理階層應指派下列責任及權限：

(a) 確保資訊安全管理系統符合本標準之要求事項。

(b) 向最高管理階層報告資訊安全管理系統之績效。

備考：最高管理階層亦可指派報告組織內資訊安全管理系統績效之責任及權限。

6. 規劃

6.1 因應風險及機會之行動

6.1.1 一般要求

於規劃資訊安全管理系統時，組織應考量 4.1 所提及之議題及 4.2 所提及的要求事項，並決定需因應之風險及機會，以達成下列事項：

(a) 確保資訊安全管理系統能達成其預期成果。

(b) 預防或減少非所欲之影響。

(c) 達成持續改善。

組織應規劃下列事項：

(d) 因應此等風險及機會之行動。及

(e) 執行下列事項之方法：

(1) 將各項行動整合及實作於其資訊安全管理系統過程中。

(2) 評估此等行動之有效性。

6.1.2 資訊安全風險評鑑

組織應定義及應用資訊安全風險評鑑過程於下列事項中：

(a) 建立及維持包括下列準則之資訊安全風險準則：

(1)風險接受準則。及

(2)執行資訊安全風險評鑑之準則。

(b) 確保重複之資訊安全風險評鑑產生一致、有效及可比較的結果。

(c) 識別資訊安全風險：

(1) 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與喪失資訊之機密性、完整性及可用性相關聯的風險。及

(2) 識別風險當責者。

(d) 分析資訊安全風險：

(1) 評鑑若 6.1.2(c)(1)中所識別之風險實際發生時，可能導致的潛在後果。

(2) 評鑑 6.1.2(c)(1)中所識別之風險發生的實際可能性。及

(3) 判定風險等級。

(e) 評估資訊安全風險：

(1) 以 6.1.2(a)中所建立之風險準則，比較風險分析結果。及

(2) 訂定已分析風險之風險處理優先序。

組織應保存關於資訊安全風險評鑑過程之文件化資訊。

6.1.3 資訊安全風險處理

組織應定義並應用資訊安全風險處理過程，以達成下列事項：

(a) 考量風險評鑑結果，選擇適切之資訊安全風險處理選項。

(b) 對所選定資訊安全風險處理選項，決定所有必須實作之控制措施。

備考 1. 組織可依要求設計控制措施，或由任何來源識別之。

(c) 比較上述 6.1.3(b)中所決定之控制措施與附錄 A 中者，並查證未忽略必要的控制措施。

備考 2. 附錄 A 包含可能之資訊安全控制措施清單。本標準之使用者參照附錄 A，以確保未忽略必要的資訊安全控制措施。

備考 3. 附錄 A 中所列之各項資訊安全控制措施並未盡列，故可能需要包括額外的資訊安全控制措施。

(d) 產生適用性聲明，包含下列各項：

- 必要之控制措施(參照 6.1.3(b)及(c))。
- 納入之衡量理由。

— 是否實作必要之控制措施。及

— 排除任何附錄 A 控制措施之衡量理由。

(e) 制定資訊安全風險處理計畫。及

(f) 取得風險擁有者對資訊安全風險處理計畫之核准，以及對剩餘資訊安全風險的接受。

組織應保存關於資訊安全風險處理過程之文件化資訊。

備考 4. 本標準中之資訊安全風險評鑑及處理過程與 CNS 31000[5]內，提供的原則及通用指導綱要調和。

6.2 資訊安全目標及其達成之規劃

組織應於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) 可量測(若可行)。

(c) 考量適用之資訊安全要求事項，以及風險評鑑及風險處理的結果。

(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。

組織應保存關於資訊安全目標之文件化資訊。

於規劃如何達成資訊安全目標時，組織應決定下列事項：

(h) 待辦事項。

(i) 所要求資源。

(j) 負責人員。

(k) 完成時間。及

(l) 結果之評估方式。

6.3 變更之規劃

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。

7. 支援

7.1 資源

組織應決定並提供建立、實作、維持及持續改善資訊安全管理系統所需之資源。

7.2 能力

組織應採取下列措施：

(a) 決定於組織控制下執行工作，影響其資訊安全績效人員之必要能力。

(b) 確保此等人員於適切教育、訓練或經驗之基礎上能勝任。

(c) 於適用時，採取行動取得必要能力，並評估所採取行動之有效性。

(d) 保存適切之文件化資訊，作為勝任之證據。

備考： 適用之行動可能包括，例：對現有員工提供訓練、指導或重新指派，或是雇用或約用勝任人員。

7.3 認知

於組織控管下，執行工作之人員應認知下列事項：

(a) 資訊安全政策。

(b) 其對資訊安全管理系統有效性之貢獻，包括改善的資訊安全績效之益處。及

(c) 未遵循資訊安全管理系統要求事項之可能後果。

7.4 溝通或傳達

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。

7.5 文件化資訊

7.5.1 一般要求

組織之資訊安全管理系統應包括下列內容：

(a) 本標準要求之文件化資訊。及

(b) 由組織所決定對資訊安全管理系統有效性，必要之文件化資訊。

備考：各組織之資訊安全管理系統文件化資訊內容，可能因下列因素而異：

(1) 組織規模，以及其活動之型式、過程、產品及服務。

(2) 各過程及其互動之複雜度。及

(3) 人員之能力。

7.5.2 制定及更新

於制定及更新文件化資訊時，組織應確保適切之下列項目：

(a) 識別及描述(例：標題、日期、作者或參引號碼)。

(b) 格式(例：語言、軟體版本、圖形)及媒體(例：紙本、電子)。及

(c) 合宜性及適切性之審查及核可。

7.5.3 文件化資訊之控制

應控制資訊安全管理系統及本標準要求之文件化資訊，以確保下列事項：

(a) 其於需要處及需要時為可用及適用。及

(b) 其受適切保護(例：防止喪失機密性、不當使用或喪失完整性)。

為控制文件化資訊，組織應於適用時，闡明下列活動：

(c) 派送、存取、檢索及使用。

(d) 儲存及保存，包括可讀性之保存。及

(e) 變更之控制(例：版本控制)。

(f) 留存及屆期處置(retention and disposition)。

於適切時，應識別及控制由組織所決定對資訊安全管理系統之規劃及運作為必要之外部來源的文件化資訊。

備考： 存取可能意味關於文件化資訊僅可檢視之許可，或檢視及變更文件化資訊的許可及權限等之決策。

8. 運作

8.1 運作之規劃及控制

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 節中所決定的行動：

— 建立過程之準則。

— 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。

8.2 資訊安全風險評鑑

組織應依規劃之期間，或當提議或發生重大變更時，考量 6.1.2(a)所建立之準則，執行資訊安全風險評鑑。

組織應保存資訊安全風險評鑑結果之文件化資訊。

8.3 資訊安全風險處理

組織應實作資訊安全風險處理計畫。

組織應保存資訊安全風險處理結果之文件化資訊。

9. 績效評估

9.1 監督、量測、分析及評估

組織應決定下列事項：

(a) 需要監督及量測之事項，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的結果。

(c) 應執行監督及量測之時間。

(d) 應執行監督及量測之人員。

(e) 監督及量測結果應分析及評估之時間。

(f) 應執行分析及評估此等結果之人員。

應具備文件化資訊，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。

9.2 內部稽核

9.2.1 一般要求

組織應依規劃之期間施行內部稽核，以提供資訊安全管理系統的下列資訊：

(a) 是否符合下列事項：

(1) 組織本身對其資訊安全管理系統之要求事項。

(2) 本標準之要求事項。

(b) 是否有效實作及維持。

9.2.2 內部稽核計畫

組織應規劃、建立、實作及維持稽核計畫，包括頻率、方法、責任、規劃要求事項及報告。

於建立內部稽核計畫時，組織應考量所關切過程之重要性及先前稽核的結果。

組織應採取下列作為：

(a) 定義各稽核之稽核準則及稽核範圍。

(b) 選擇稽核員及施行稽核，以確保稽核過程之客觀性及公平性。

(c) 確保稽核之結果對相關管理階層報告。

應具備文件化資訊，作為稽核計畫實作及稽核結果之證據。

9.3 管理審查

9.3.1 一般要求

最高管理階層應於規劃之期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。

9.3.2 管理審查輸入

管理審查應包括對下列事項之考量：

(a) 過往管理審查之決議的處理狀態。

(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。

(d) 資訊安全績效之回饋，包括下列之趨勢：

(1) 不符合事項及矯正措施。

(2) 監督及量測結果。

(3) 稽核結果。

(4) 資訊安全目標之達成。

(e) 關注方之回饋。

(f) 風險評鑑結果及風險處理計畫之狀態。

(g) 持續改善之機會。

9.3.3 管理審查結果

管理審查之結果應包括與持續改善機會相關的決策，以及任何對資訊安全管理系統變更之需要。

應具備文件化資訊，以作為管理審查結果之證據。

10. 改善

10.1 持續改善

組織應持續改善資訊安全管理系統之合宜性、適切性及有效性。

10.2 不符合事項及矯正措施

不符合事項發生時，組織應有下列作為：

(a) 對不符合事項反應，並於適用時，採取下列作為：

(1) 採取行動，以控制並矯正之。

(2) 處理其後果。

(b) 藉由下列作為，評估對消除不符合事項之原因的行動之需要，使其不再發生且不於他處發生：

(1) 審查不符合事項。

(2) 判定不符合事項之原因。及

(3) 判定是否有類似之不符合事項存在，或可能發生。

(c) 實作所有所需行動。

(d) 審查所有所採取矯正措施之有效性。

(e) 必要時，對資訊安全管理系統進行變更。

矯正措施應切合所遇到不符合事項之影響。

應具備文件化資訊，以作為下列事項之證據：

(f) 不符合事項之性質及後續採取的所有行動。

(g) 所有矯正措施之結果。

附錄 A
(規定)
資訊安全控制措施參引

表 A.1 所列之各項資訊安全控制措施，乃直接取自 CNS 27002[1]之第 5 節至第 8 節，並與之調和，且於內文中與 6.1.3 一起使用。

表 A.1　資訊安全控制措施

5	**組織控制措施**	
5.1	**資訊安全政策**	**控制措施** 資訊安全政策及主題特定政策應予以定義、由管理階層核可、發布、傳達予相關人員及相關關注方，且其係知悉，並依規劃期間及發生重大變更時審查。
5.2	**資訊安全之角色及責任**	**控制措施** 應依組織需要，定義並配置資訊安全之角色及責任。
5.3	**職務區隔**	**控制措施** 衝突之職務及衝突的責任範圍應予以區隔。
5.4	**管理階層責任**	**控制措施** 管理階層應要求所有人員，依組織所建立資訊安全政策、主題特定政策及程序，實施資訊安全。
5.5	**與權責機關之聯繫**	**控制措施** 組織應建立並維持與相關權責機關之聯繫。
5.6	**與特殊關注群組之聯繫**	**控制措施** 組織應建立並維持與各特殊關注群組或其他各專家安全論壇及專業協會之聯繫。
5.7	**威脅情資**	**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。
5.8	**專案管理之資訊安全**	**控制措施** 資訊安全應整合入專案管理中。
5.9	**資訊及其他相關聯資產之清冊**	**控制措施** 應製作並維護資訊及其他相關聯資產(包括擁有者)之清冊。
5.10	**可接受使用資訊及其他相關聯資產**	**控制措施** 應識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序。
5.11	**資產之歸還**	**控制措施** 適切時，人員及其他關注方於其聘用、契約或協議變更或終止時，應歸還其持有之所有組織資產。

表 A.1　資訊安全控制措施(續)

5.12	**資訊之分類分級**	**控制措施** 資訊應依組織之資訊安全需要，依機密性、完整性、可用性及相關關注方要求事項分類分級。
5.13	**資訊之標示**	**控制措施** 應依組織所採用之資訊分類分級方案，發展及實作一套適切的資訊標示程序。
5.14	**資訊傳送**	**控制措施** 應備妥資訊傳送規則、程序或協議，用於組織內及組織與其他各方間之所有型式的傳送設施。
5.15	**存取控制**	**控制措施** 應依營運及資訊安全要求事項，建立並實作對資訊及其他相關聯資產之實體及邏輯存取控制的規則。
5.16	**身分管理**	**控制措施** 應管理身分之整個生命週期。
5.17	**鑑別資訊**	**控制措施** 鑑別資訊之配置及管理應由管理過程控制，包括告知人員關於鑑別資訊的適切處理。
5.18	**存取權限**	**控制措施** 應依組織之存取控制的主題特定政策及規則，提供、審查、修改及刪除對資訊及其他相關聯資產之存取權限。
5.19	**供應者關係中之資訊安全**	**控制措施** 應定義並實作過程及程序，管理與供應者產品或服務之使用相關聯的資訊安全風險。
5.20	**於供應者協議中闡明資訊安全**	**控制措施** 應依供應者關係之型式，建立相關的資訊安全要求事項，並與各供應者議定。
5.21	**管理ICT供應鏈中之資訊安全**	**控制措施** 應定義並實作過程及程序，管理與ICT產品及服務供應鏈相關聯之資訊安全風險。
5.22	**供應者服務之監視、審查及變更管理**	**控制措施** 組織應定期監視、審查、評估及管理供應者資訊安全實務作法及服務交付之變更。
5.23	**使用雲端服務之資訊安全**	**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。
5.24	**資訊安全事故管理規劃及準備**	**控制措施** 組織應藉由定義、建立並溝通或傳達資訊安全事故管理過程、角色及責任，規劃並準備管理資訊安全事故。

表 A.1　資訊安全控制措施(續)

5.25	**資訊之評鑑及決策**	**控制措施** 組織應評鑑資訊安全事件，並判定是否將其歸類為資訊安全事故。
5.26	**對資訊安全事故之回應**	**控制措施** 應依書面記錄程序，回應資訊安全事故。
5.27	**由資訊安全事故中學習**	**控制措施** 應使用由資訊安全事故中所獲得之知識，強化及改善資訊安全控制措施。
5.28	**證據之蒐集**	**控制措施** 組織應建立並實作程序，用以識別、蒐集、獲取及保存與資訊安全事件相關之證據。
5.29	**中斷期間之資訊安全**	**控制措施** 組織應規劃，如何於中斷期間維持資訊安全於適切等級。
5.30	**營運持續之ICT備妥性**	**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。
5.31	**法律、法令、法規及契約要求事項**	**控制措施** 應識別、書面記錄及保持更新資訊安全相關法律、法令、法規及契約之要求事項，以及組織為符合此等要求事項的作法。
5.32	**智慧財產權**	**控制措施** 組織應實作適切程序，以保護智慧財產權。
5.33	**紀錄之保護**	**控制措施** 應保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。
5.34	**隱私及PII保護**	**控制措施** 組織應依適用之法律、法規及契約的要求事項，識別並符合關於隱私保護及PII保護之要求事項。
5.35	**資訊安全之獨立審查**	**控制措施** 應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全的作法及其實作(包括人員、過程及技術)。
5.36	**資訊安全政策、規則及標準之遵循性**	**控制措施** 應定期審查組織資訊安全政策、主題特定政策、規則及標準之遵循性。
5.37	**書面記錄之運作程序**	**控制措施** 應書面記錄資訊處理設施之運作程序，並使所有需要的人員均可取得。

表 A.1　資訊安全控制措施(續)

6	**人員控制措施**	
6.1	**篩選**	**控制措施** 對所有成為員工之候選者，應於其加入組織前，進行背景查證調查，且持續進行，同時將適用的法律、法規及倫理納入考量，並宜相稱於營運要求事項，其將存取之資訊的分類分級及所察覺之風險。
6.2	**聘用條款及條件**	**控制措施** 聘用契約協議應敘明人員及組織對資訊安全之責任。
6.3	**資訊安全認知及教育訓練**	**控制措施** 組織及相關關注方之人員，均應接受與其工作職能相關的組織資訊安全政策、主題特定政策及程序之適切資訊安全認知及教育訓練，並定期更新。
6.4	**獎懲過程**	**控制措施** 應明確訂定並傳達獎懲過程，以對違反資訊安全政策之人員及其他相關關注方採取行動。
6.5	**聘用終止或變更後之責任**	**控制措施** 應對相關人員及其他關注方定義、施行並傳達於聘用終止或變更後，仍保持有效之資訊安全責任及義務。
6.6	**機密性或保密協議**	**控制措施** 反映組織對資訊保護之需要的機密性或保密協議，應由人員及其他相關關注方，識別、書面記錄、定期審查及簽署。
6.7	**遠端工作**	**控制措施** 應實作安全措施，當人員於遠端工作時，保護於組織場所外存取、處理或儲存之資訊。
6.8	**資訊安全事件通報**	**控制措施** 組織應提供機制，供人員透過適切之管道，及時通報所觀察到或可疑的資訊安全事件。
7	**實體控制措施**	
7.1	**實體安全周界**	**控制措施** 應定義及使用安全周界，以保護收容資訊及其他相關聯資產之區域。
7.2	**實體進入**	**控制措施** 保全區域應藉由適切之進入控制措施及進出點加以保護。
7.3	**保全辦公室、房間及設施**	**控制措施** 應設計辦公室、房間及設施之實體安全並實作之。
7.4	**實體安全監視**	**控制措施** 應持續監視場所，防止未經授權之實體進出。

表 A.1　資訊安全控制措施(續)

7.5	防範實體及環境威脅	控制措施 應設計並實作防範實體及環境威脅(諸如天然災害及其他對基礎設施之蓄意或非蓄意的實體威脅)之措施。
7.6	於安全區域內工作	控制措施 應設計並實作於安全區域內工作之安全措施。
7.7	桌面淨空及螢幕淨空	控制措施 應定義對紙本及可移除式儲存媒體之桌面淨空規則，以及對資訊處理設施的螢幕淨空規則，並適切實施之。
7.8	設備安置及保護	控制措施 設備應安全安置並受保護。
7.9	場所外資產之安全	控制措施 應保護場域外資產。
7.10	儲存媒體	控制措施 儲存媒體應依組織之分類分級方案及處置要求事項，於其獲取、使用、運送及汰除的整個生命週期內進行管理。
7.11	支援之公用服務事業	控制措施 應保護資訊處理設施免於電源失效，以及因支援之公用服務事業失效，所導致的其他中斷。
7.12	佈纜安全	控制措施 應保護傳送電源、資料或支援資訊服務之纜線，以防範竊聽、干擾或破壞。
7.13	設備維護	控制措施 應正確維護設備，以確保資訊之可用性、完整性及機密性。
7.14	設備汰除或重新使用之保全	控制措施 應查證包含儲存媒體之設備項目，以確保於汰除或重新使用前，所有敏感性資料及具使用授權的軟體已移除或安全覆寫。
8	技術控制措施	
8.1	使用者端點裝置	控制措施 應保護儲存於使用者端點裝置、由使用者端點裝置處理或經由使用者端點裝置可存取之資訊。
8.2	特殊存取權限	控制措施 應限制並管理特殊存取權限之配置及使用。
8.3	資訊存取限制	控制措施 應依已建立之關於存取控制的主題特定政策，限制對資訊及其他相關聯資產之存取。
8.4	對原始碼之存取	控制措施 應適切管理對原始碼、開發工具及軟體函式庫之讀寫存取。

表 A.1　資訊安全控制措施(續)

8.5	**安全鑑別**	**控制措施** 安全鑑別技術及程序應依資訊存取限制及關於存取控制之主題特定政策實作。
8.6	**容量管理**	**控制措施** 資源之使用應受監視及調整，以符合目前容量要求及預期容量要求。
8.7	**防範惡意軟體**	**控制措施** 應實作防範惡意軟體之措施，並由適切的使用者認知支援之。
8.8	**技術脆弱性管理**	**控制措施** 應取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適切措施。
8.9	**組態管理**	**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)。
8.10	**資訊刪除**	**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。
8.11	**資料遮蔽**	**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。
8.12	**資料洩露預防**	**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。
8.13	**資訊備份**	**控制措施** 應依議定之關於備份的主題特定政策，維護資訊、軟體及系統之備份複本，並定期測試之。
8.14	**資訊處理設施之多備**	**控制措施** 資訊處理設施之實作應具充分多備(redundancy)，以符合可用性之要求事項。
8.15	**存錄**	**控制措施** 記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。
8.16	**監視活動**	**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。
8.17	**鐘訊同步**	**控制措施** 組織所使用資訊處理系統之鐘訊，應與經認可的時間源同步。
8.18	**具特殊權限公用程式之使用**	**控制措施** 應限制並嚴密控制可能篡越系統及應用程式之控制措施的公用程式之使用。

表 A.1　資訊安全控制措施(續)

8.19	**運作中系統之軟體安裝**	**控制措施** 應實作各項程序及措施，以安全管理對運作中系統安裝軟體。
8.20	**網路安全**	**控制措施** 應受保全、管理及控制網路與網路裝置，以保護系統及應用程式中之資訊。
8.21	**網路服務之安全**	**控制措施** 應識別、實作及監視網路服務之安全機制、服務等級及服務要求事項。
8.22	**網路區隔**	**控制措施** 應區隔組織網路中各群組之資訊服務、使用者及資訊系統。
8.23	**網頁過濾**	**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。
8.24	**密碼技術之使用**	**控制措施** 應定義並實作有效使用密碼技術之規則(包括密碼金鑰管理)。
8.25	**安全開發生命週期**	**控制措施** 應建立並施行安全開發軟體及系統之規則。
8.26	**應用系統安全要求事項**	**控制措施** 開發或獲取應用系統時，應識別、規定並核可資訊安全要求事項。
8.27	**安全系統架構及工程原則**	**控制措施** 應建立、書面記錄及維護工程化安全系統之原則，並套用於所有資訊系統開發活動。
8.28	**安全程式設計**	**控制措施** 軟體開發應施行安全程式設計原則。
8.29	**開發及驗收中之安全測試**	**控制措施** 應於開發生命週期中定義並實作安全測試過程。
8.30	**委外開發**	**控制措施** 組織應指引、監視及審查與委外系統開發相關之活動。
8.31	**開發、測試與運作環境之區隔**	**控制措施** 應區隔開發環境、測試環境與生產環境，並保全之。
8.32	**變更管理**	**控制措施** 資訊處理設施及資訊系統之變更，應遵循變更管理程序。
8.33	**測試資訊**	**控制措施** 應適切選擇、保護及管理測試資訊。
8.34	**稽核測試期間資訊系統之保護**	**控制措施** 涉及運作中系統之評鑑的稽核測試及其他保證活動，應於測試者與適切管理階層間規劃並議定。

名詞對照

−A−	
acceptance	驗收；接受
access control	存取控制
access right	存取權限
adequacy	適切性
agreement	協議
application system	應用系統
approach	作法
aspect	層面
assessment	評鑑
asset	資產
audit	稽核
authentication	鑑別
authorization	授權
availability	可用性
awareness	認知
−B−	
backup	備份
business continuity management	營運持續管理
−C−	
channel	管道；通道
classification	分類分級
clear desk	桌面淨空
clear screen	螢幕淨空
communication	溝通或傳達
compliance	遵循性；遵循
confidentiality	機密性
competence	能力
contract	契約
control	控制措施
criteria	準則
cryptography	密碼學
cybersecurity	網宇安全

−D−	
development	發展；開發
disaster	災害
disciplinary	懲處
disposal	汰除；棄置；作廢
disruption	中斷
duty	職務；義務
−E−	
employment	聘用
equipment	設備
evaluation	評估
event	事件
evidence	證據
−F−	
facility	設施
forum	論壇
framework	框架
fraud	詐欺
−G−	
generic	通用
guideline	指導綱要
−H−	
handling	處置
hazard	危害
−I−	
identification	識別
identity	身分；識別資訊
impact	衝擊
implementation	實作
incident	事故
information and communication technology, ICT	資通訊技術
information security	資訊安全

integrity	完整性
interested party	關注方
intellectual property right, IPR	智慧財產權
information security management system, ISMS	資訊安全管理系統
inventory	清冊
−K−	
key management	金鑰管理
−L−	
label	標籤
labelling	標示
legibility	可讀性
log	日誌；存錄
logging	存錄
−M−	
maintenance	維持；維護
malware	惡意軟體
mechanism	機制
media	媒體
misuse	誤用
mobile device	行動裝置
monitor	監視；監督
−N−	
nonconformity	不符合事項
non-disclosure agreement	保密協議
−O−	
objective	目標
obligation	義務
outsource	委外
−P−	
password	通行碼
perimeter	周界
personal identifiable information, PII	個人可識別資訊

personnel	人員
policy	政策
premise	場所
preservation	保存
privacy	隱私
privacy protection	隱私保護
privilege	特殊權限
procedure	程序
process	過程；處理；處理過程

−R−

registration	註冊
remote working	遠端工作
responsibility	責任
retention	留存；保存
review	審查
risk	風險
risk acceptance	風險接受
risk analysis	風險分析
risk assessment	風險評鑑
risk evaluation	風險評估
risk management	風險管理
risk owner	風險當責者
risk treatment	風險處理

−S−

scheme	方案
screening	篩選
segregation	區隔
source code	原始碼
statement of applicability	適用性聲明
suitability	合宜性
supplier	供應者
supply chain	供應鏈
synchronization	同步

−T−

teleworking	遠距工作
terms and conditions	條款及條件
threat	威脅
threat intelligence	威脅情資
−U−	
unattended user equipment	無人看管之使用者設備
utility	公用設施；公用程式；公用事業
−V−	
verification	查證
vulnerability	脆弱性
−W−	
weakness	弱點

參考資料

[1] CNS 27002 資訊安全、網宇安全及隱私保護－資訊安全控制措施

[2] CNS 27003 資訊技術－安全技術－資訊安全管理系統實作指引

[3] CNS 27004 資訊技術－安全技術－資訊安全管理－量測

[4] CNS 27005 資訊技術－安全技術－資訊安全風險管理

[5] CNS 31000 風險管理－指導綱要

相對應國際標準

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

修訂日期

第一次修訂：96 年 10 月 24 日

第二次修訂：103 年 04 月 24 日