恆遠白話系列 · 資安篇

CNS 27001
白話讀本

一份給中小企業老闆與團隊的資訊安全管理系統（ISMS）完整地圖。
本文七大條 + 附錄A 九十三項控制措施，每一項都翻成一句人話。

查核通過的公司，都在做這些事

7	4	93	11
本文條款（第4至10節）	控制主題（組織/人員/實體/技術）	附錄A控制措施	新版新增措施

恆遠數位科技有限公司 | foreverwebs.com

這份標準到底在講什麼

CNS 27001 是台灣的國家標準，內容等同國際標準 ISO/IEC 27001:2022，全名是「資訊安全管理系統（ISMS）要求事項」。一句話總結：它要求一間組織把資訊安全**做成一套會自己運轉的管理制度**，有政策、有風險評估、有紀錄、有稽核、有改善，而且高層要親自負責。

> **先破除三個最常見的誤會：**

誤會一：「27001 就是一張證書。」

證書是找驗證機構稽核後發的那張紙；標準本身是一套「怎麼把資安管好」的方法。沒有證書的公司一樣可以（也應該）依標準把制度做實，政府契約常見的「符合 CNS 27001」要求的正是後者：拿得出文件與紀錄，而非牆上那張紙。

誤會二：「管理系統是一套要採購的軟體。」

ISMS 的「系統」指的是管理制度：政策、流程、責任分工、紀錄與改善循環。它存在於文件與日常運作裡，跟買不買某套軟體無關。

誤會三：「93 項控制措施每一項都得做到。」

附錄A是一份「檢查是否遺漏」的清單。標準要求先做風險評鑑，再依風險決定哪些措施適用，寫成「適用性聲明書（SoA）」。不適用的可以排除，但要說得出理由。小公司照樣能合規，重點在誠實面對自己的風險。

> **整套標準的骨架是 PDCA 循環：**規劃（Plan）→ 執行（Do）→ 檢核（Check）→ 行動（Act）。下一頁的本文七大條，就是把這個循環拆成可以稽核的具體要求。

> **看懂編號，先記兩件事：**
> ①　本文其實有第1至10條，但第1至3條是適用範圍、引用標準與名詞定義，屬前置說明、無稽核要求，實質要求從**第4條起跳**，所以大家慣稱「本文七大條」。這是 ISO 管理系統標準共用的調和結構，9001、14001 也長一樣。
> ②　附錄A的93項控制措施引用自另一份標準 ISO 27002 的第5至8章，編號原樣搬入，因此從 **5 開頭**，嚴謹寫法會加上「A.」字首（如 A.5.1）。請留意：本文第5條「領導」與附錄A的5.1「資訊安全政策」是**完全不同的東西**，前者是必答的制度條款，後者是依風險選用的控制措施。

本文七大條：管理系統的骨架

第4至10節是標準的「必答題」，申請驗證時每一條都會被稽核，不能排除。用白話讀是這樣：

4 **組織全景** Plan

搞清楚自己是誰：公司內外在環境、利害關係人（客戶、主管機關、員工）各要什麼，然後把 ISMS 的範圍畫清楚，哪些系統與部門在圈內。

5 **領導** Plan

老闆親自下場：管理階層要承諾資源、簽署資訊安全政策、指派角色與權責。資安是治理議題，推給資訊人員單打獨鬥就註定失敗。

6 **規劃** Plan

做風險評鑑：盤點資產、找出威脅、評估衝擊，決定怎麼處理（降低、移轉、避免、接受），並訂出可衡量的資安目標。2022 年版新增 6.3：要動 ISMS 的任何變更，都得先規劃再動手。

7 **支援** Do

給糧草：人力預算要到位、人員能力要培養、全員要有資安認知、內外溝通有規則、文件有版本管制。

8 **運作** Do

真的去做：把第6節規劃的風險處理落地執行，定期重跑風險評鑑，過程留下紀錄。

9 **績效評估** Check

自己考自己：監視與量測指標、辦內部稽核、管理階層定期開審查會議，檢視制度有沒有真的在運轉。

10 **改善** Act

愈跑愈好：發現不符合事項要矯正並追根因，制度持續改善，循環回到第4節。

> **讀附錄A之前先記住：**接下來的 93 項控制措施分成四大主題，編號 5 開頭是組織面、6 開頭是人員面、7 開頭是實體環境面、8 開頭是技術面。右欄的白話是幫助理解的摘寫，正式條文文字以標準本文為準。

附錄A・組織控制措施 37 項

制度、資產、供應商與事故管理的遊戲規則

5.1	**資訊安全政策**	把公司的資安遊戲規則白紙黑字寫下來，管理階層核可，全員知悉。
5.2	**資訊安全角色及責任**	誰負責什麼，指名道姓寫清楚。
5.3	**職務區隔**	關鍵權限拆給不同人，避免一人全包、球員兼裁判。
5.4	**管理階層責任**	主管帶頭要求所有人照政策與程序做事。
5.5	**與權責機關之聯繫**	知道出事要通報誰，平常就建立好聯絡窗口。
5.6	**與特殊關注團體之聯繫**	參與資安社群與論壇，情報管道不斷線。
5.7	**威脅情資** 新增	蒐集並分析攻擊趨勢，先知道別人正在怎麼被打。
5.8	**專案管理中之資訊安全**	每個專案立案時就把資安需求放進去。
5.9	**資訊及其他相關資產之清冊**	家裡有什麼要有清單：系統、資料、設備都造冊並指定負責人。
5.10	**資訊及其他相關資產之可接受使用**	公司的設備與資料可以怎麼用、不能怎麼用，說清楚。
5.11	**資產歸還**	離職或換約時，電腦、帳號、資料一樣不漏收回來。
5.12	**資訊之分類分級**	依機密性把資訊分級：機密、內部、公開。
5.13	**資訊之標示**	分級之後要標示出來，讓經手的人一眼看懂。
5.14	**資訊傳送**	傳資料的管道與規則要安全，對內對外都一樣。
5.15	**存取控制**	誰能看什麼、進哪個系統，依業務需要給，不多不少。
5.16	**身分管理**	一人一身分，帳號的產生與註銷全程列管。
5.17	**鑑別資訊**	密碼、金鑰這類鑑別資訊的發放與保管有規矩。
5.18	**存取權限**	權限的授予、調整、收回走流程並定期盤點。
5.19	**供應者關係中之資訊安全**	跟廠商往來之前，先想清楚資安風險怎麼管。
5.20	**供應者協議中之資訊安全**	把資安要求寫進合約，口頭承諾不算數。
5.21	**ICT供應鏈之資訊安全管理**	上游的上游也要管，元件與服務來源看得見。
5.22	**供應者服務之監視、審查及變**	廠商的服務要持續盯、定期審、變更要知會。

	更管理	
5.23	**使用雲端服務之資訊安全** 新增	上雲的選用、使用、退場規則先講好。
5.24	**資安事故管理之規劃與準備**	出事前先把劇本、角色、流程演練好。
5.25	**資安事件之評估與決策**	判斷這是小事件還是要升級的大事故。
5.26	**資安事故之回應**	照既定程序處理事故，不靠臨場發揮。
5.27	**從資安事故中學習**	每次出事都變成教材，回頭補強控制。
5.28	**證據之蒐集**	證據的取得與保存方法要正確，日後調查才站得住。
5.29	**營運中斷期間之資訊安全**	停電、停機、災難期間，安全水準不能跟著停。
5.30	**營運持續之ICT備妥性** 新增	系統斷了多快要恢復，先定目標並準備好。
5.31	**法律、法規及契約要求事項**	適用哪些法規與合約義務，逐一盤點並遵循。
5.32	**智慧財產權**	軟體授權、字型、素材版權不能踩線。
5.33	**紀錄之保護**	重要紀錄防竄改、防遺失、依年限保存。
5.34	**隱私及個資保護**	依個資法等要求保護個人資料。
5.35	**資訊安全之獨立審查**	定期由非當事人檢視制度是否有效。
5.36	**資訊安全政策、規則及標準之遵循**	檢查大家是否真的照規定做。
5.37	**書面作業程序**	操作步驟寫成文件，不依賴某個人的腦袋。

附錄A・人員控制措施 8 項

從報到第一天到離職之後的人的管理

6.1	**篩選**	用人之前做適當的背景查核。
6.2	**聘用條款及條件**	勞動契約寫明資安責任與義務。
6.3	**資訊安全認知、教育及訓練**	定期教育訓練，讓全員知道自己該做什麼。
6.4	**懲處程序**	違反資安規定時，有明確且公正的處理程序。
6.5	**聘用終止或變更後之責任**	離職之後，保密義務依然有效並讓當事人知道。
6.6	**保密或不揭露協議**	NDA 簽好簽滿，內容定期檢視更新。
6.7	**遠距工作**	在家或外部工作的設備、連線與環境有規範。
6.8	**資訊安全事件通報**	人人知道看到異常要往哪裡報、多快報。

附錄A・實體控制措施 14 項

門禁、機房、設備與環境的看得見的安全

7.1	**實體安全周界**	劃出需要保護區域的界線。
7.2	**實體進入**	門禁管制與訪客登記，該鎖的門要鎖。
7.3	**辦公室、房間及設施之安全防護**	重要空間妥善上鎖與防護。
7.4	**實體安全監視** 新增	以監視器、警報器持續看守重要區域。
7.5	**防範實體及環境威脅**	火災、水患、地震等威脅預先設防。
7.6	**於安全區域內工作**	機房等敏感區域的作業守則。
7.7	**桌面淨空及螢幕淨空**	下班桌面不留敏感文件，離座就鎖螢幕。
7.8	**設備之放置及保護**	設備擺放位置適當並妥善保護。
7.9	**場所外資產之安全**	帶出公司的筆電、手機、文件要顧好。
7.10	**儲存媒體**	隨身碟與硬碟的使用、搬運、銷毀有規則。
7.11	**支援之公用事業**	電力、空調、網路要穩定並有備援。
7.12	**佈纜安全**	線路防竊聽、防干擾、防破壞。
7.13	**設備維護**	設備定期保養，送修時防止資料外洩。
7.14	**設備之安全汰除或再使用**	報廢或轉用前，先把資料徹底清乾淨。

附錄A・技術控制措施 34 項

系統、網路、開發與監控的技術防線

8.1	**使用者端點設備**	員工的電腦與手機統一納管防護。
8.2	**特殊存取權限**	管理員權限少發、嚴管、定期檢視。
8.3	**資訊存取限制**	系統內依角色限制可存取的資料範圍。
8.4	**原始碼之存取**	程式碼與開發工具管好誰能碰。
8.5	**安全鑑別**	登入機制要夠強，例如多因子驗證。
8.6	**容量管理**	效能與空間提前規劃，別等爆了才知道。
8.7	**防範惡意軟體**	防惡意程式的技術措施加上員工警覺。
8.8	**技術脆弱性管理**	定期弱點掃描，及時修補漏洞。
8.9	**組態管理** 新增	系統設定標準化並防止未經授權的更動。
8.10	**資訊刪除** 新增	不再需要的資料依規定確實刪除。
8.11	**資料遮蔽** 新增	測試或展示用的資料先去識別化。
8.12	**資料洩漏預防** 新增	部署機制防止敏感資料被帶出去。
8.13	**資訊備份**	定期備份，而且要實際演練還原。
8.14	**資訊處理設施之備援**	重要系統有備援，不留單點故障。
8.15	**存錄**	系統日誌完整留存並保護不被竄改。
8.16	**監視活動** 新增	持續監控網路與系統的異常行為。
8.17	**時鐘同步**	所有系統對時，日誌時間才對得起來。
8.18	**特殊權限公用程式之使用**	可繞過控制的系統工具嚴格管制。
8.19	**運作中系統之軟體安裝**	正式環境不能隨便安裝軟體。
8.20	**網路安全**	網路設備與流量的安全管理。
8.21	**網路服務之安全**	使用的網路服務其安全要求要明確。
8.22	**網路之區隔**	內外網、不同信任等級的網段分開。
8.23	**網頁過濾** 新增	阻擋惡意與不當網站的存取。
8.24	**密碼學之使用**	加密演算法與金鑰管理訂有規則。

8.25	**安全開發生命週期**	從設計到上線，每個階段都想資安。
8.26	**應用系統安全要求事項**	需求階段就定義系統的安全需求。
8.27	**安全系統架構及工程原則**	架構設計遵循安全原則，例如最小權限。
8.28	**安全程式設計** 新增	撰碼遵循安全規範，防注入、防越權。
8.29	**開發及驗收中之安全測試**	上線之前執行安全測試。
8.30	**委外開發**	外包開發的資安要求一樣要管到。
8.31	**開發、測試及正式環境之區隔**	三種環境分開，資料不混用。
8.32	**變更管理**	系統改動走流程、經核可、留紀錄。
8.33	**測試資訊**	測試資料的挑選與保護有規範。
8.34	**稽核測試期間資訊系統之保護**	稽核與檢測作業不能危及正式系統。

中小企業從零開始的務實路線

看完 93 項先別緊張，合規的順序有跡可循。以下是我們陪客戶走過、也在自己公司實作的起步五步：

第一步・盤點資產與風險（對應本文第6節、措施5.9）
列出你的系統、資料與設備，挑出最怕出事的十五到二十項，寫成風險評鑑清冊。這一份文件是整套制度的心臟。

第二步・寫一頁資安政策，老闆簽名（對應本文第5節、措施5.1）
一頁就夠。宣示原則、指定資安負責人、要求全員遵守。

第三步・把五件日常做實（措施5.15、6.6、8.8、8.13、6.8）
權限控管、保密協議、定期弱掃修補、備份加還原演練、事件通報流程。這五件涵蓋了多數真實事故的防線。

第四步・留紀錄（措施5.33、5.37、8.15）
做了就要留痕跡：權限異動、備份還原、教育訓練、事件處理。查核時能翻出來的紀錄，才是能力的證明。

第五步・每季自我檢核一次（對應本文第9、10節）
開一場小會，檢視風險有沒有變、措施有沒有跟上，把發現的問題排進改善。循環轉起來，制度就活了。

版本與依據：本讀本依 CNS 27001:2023（技術內容等同 ISO/IEC 27001:2022）之架構編寫；附錄A控制措施共93項，分為組織（37）、人員（8）、實體（14）、技術（34）四大主題，其中11項為2022年版新增。文中各條白話說明為本公司之理解與摘寫，僅供學習參考，正式條文以經濟部標準檢驗局公告之標準文本為準。