ISO/IEC 27001資訊安全管理系統（ISMS）主導稽核員認知

總會諮詢顧問 廖建利

ISO/IEC 27001是國際公認的資訊安全管理系統（**ISMS, Information Security Management System**）標準，提供一套結構化、系統化的框架，協助組織建立、執行、維護與持續改善資訊安全管理機制，以保護資訊資產的機密性、完整性與可用性（CIA）。

一、ISO/IEC 27001 的基本架構與精神

1. 管理系統導向（Management System）

採用PDCA（Plan-Do-Check-Act）循環、持續改善。

強調資訊安全不只是技術問題，更是組織層級的治理問題。

2. 三大核心目標

- **機密性**（Confidentiality）：未授權者無法存取資訊。
- **完整性**（Integrity）：資訊未被未授權更改或破壞。
- **可用性**（Availability）：資訊在需要時能被合法存取與使用。

二、標準主要條文（Clause 4\~10）

- 條文編號4組織背景（條文內容）理解內外部議題與利害關係人需求
- 條文編號5領導統御（條文內容）管理階層承諾、角色職責分配
- 條文編號6規劃（條文內容）風險管理程序、資訊安全目標
- 條文編號7支援（條文內容）資源、人員能力、訓練、溝通與文件控管
- 條文編號8作業（條文內容）日常運作流程與控制措施執行
- 條文編號9績效評估（條文內容）稽核、監測、管理審查等績效監控
- 條文編號10改進（條文內容）不符合矯正、持續改善措施

三、附錄A控制措施（Annex A）2022版本更新

ISO/IEC 27001：2022 版將控制措施由原來的114項精簡93項，分為以下4大類別：

- 分類A.5 組織控制（說明）管理政策與流程（範例）接取控制政策、人資安全、供應商管理
- 分類A.6人員控制（說明）人員行為與角色（範例）員工訓練、資安意

識、離職程序

- 分類A.7實體控制（說明）實體空間與裝置（範例）門禁控制、設備保護、環境安全
- 分類A.8技術控制（說明） 資訊系統技術措施（範例）密碼控管、網路安全、惡意程式防護

四、導入與維運流程

1. **初期規劃：**成立ISMS專案小組、釐清導入範疇與目標、盤點資訊資產與風險。

2. **系統建置：**建立資訊安全政策與程序文件、實施控制措施、執行教育訓練與資安意識提升。

3. **稽核與改善：**定期執行內部稽核、管理審查會議、依據稽核結果執行矯正與預防措施。

五、導入效益

- **項目類別：**強化資安治理（說明）建立制度性控制機制，提升風險管理能力。
- **項目類別：**法規合規（說明）符合法令要求（如GDPR、個資法）。
- **項目類別：**信任提升（說明）對客戶、供應商展示資訊保護承諾。
- **項目類別：**事件預防與回應（說明）降低資安事件的發生率與衝擊。
- **項目類別：**提升競爭力（說明）成為國內外招標與合作加分項目。

六、與其他標準的整合性

- 國際標準ISO-27701延伸至個人資料保護（PIMS）
- 國際標準ISO-22301業務持續管理（BCMS）
- 國際標準ISO 9001品質管理系統
- 國際標準ISO-31000風險管理通用原則

七、未來趨勢與可行性

1. **與隱私法規整合：**組織越來越需要同時應對資安與隱私治理（如GDPR、台灣個資法、CCPA）。

2. **零信任架構（Zero Trust）與雲端安全納入**：**企業需將ISMS延伸至多雲與遠端架構。

3. **AI資安納入規劃**：**AI模型與訓練資料的保護將成為下一波稽核重點。

4. **自動化稽核與持續合規（Continuous Compliance）**：**導入GRC工具與自動監測機制。

八、誰應該導入ISO 27001？

1. 金融、醫療、電信、電商等高風險行業
2. 處理大量用戶資料** 的科技公司與SaaS平台
3. 想參與國際合作或供應鏈管理** 的中小企業
4. 政府機關與教育機構**（日益成為駭客目標）

主導稽核員的認知與職責

1.定義與角色：

ISO 27001主導稽核員是經過專業訓練與認證，具備主導及執行資訊安全管理系統（ISMS）第三方稽核的能力的專業人員。其主要職責是：主導稽核計畫與準備工作、領導稽核團隊執行稽核任務、評估組織對ISO 27001標準的符合性、發現問題、提出不符合事項（NCR）、撰寫稽核報告及提出改善建議。

2.核心能力：

熟悉 ISO/IEC 27001條文與實務應用、了解 ISO/IEC 27002控制措施（附錄A）、精通風險評鑑與風險處理程序、溝通與訪談技巧，尤其在面對管理階層時、領導稽核團隊的計畫與協調能力、客觀與中立的專業判斷。

3.主導稽核實務流程

（1）稽核計畫制定：與受稽單位協調，確定範疇、時程與目標。

（2）文件審查：審查ISMS 文件（政策、程序、風險評估報告等）。

（3）現場稽核執行：透過訪談、文件查核、觀察操作等確認符合性。

（4）問題紀錄與報告：發現不符合項目，區分為重大不符合（Major）與輕微不符合（Minor）。

（5）後續追蹤與改善**：確認矯正措施的有效性。

4.未來可行性與趨勢發展

4-1.國際趨勢與職涯需求

資安威脅持續演進**（如勒索軟體、社交工程），導致企業對ISO 27001導入與認證需求提高。

合規需求擴大**：GDPR、台灣的個資法、日本的APPI等法規強化對資安制度的要求。

稽核人才短缺**：主導稽核員具高度專業性，未來在顧問、內控、資安稽核職位將持續需求上升。

4-2. 數位轉型下的挑戰

雲端與遠端作業普及**：導致稽核對虛擬環境、第三方服務（如AWS、Azure）控制的要求提升。

AI應用與資安風險交織**：主導稽核員需了解AI模型使用的資訊安全風險與治理策略。

4-3. 主導稽核員的未來發展方向

結合 **ISO 27701（隱私管理）** 擴展至資料保護領域。

熟悉 **SOC 2**、**NIST CSF** 等框架，拓展跨國稽核與顧問角色。

整合**ESG中的G治理指標**，進入企業治理審查層級。

五、結語建議

若您有志於成為ISO 27001主導稽核員，建議：

1. 參加IRCA或PECB認證課程**。
2. 熟讀ISO/IEC 27001 & 27002之條文及實務案例。
3. 積累實際資訊安全管理與稽核經驗。
4. 具備風險評估、控制設計與內稽能力，強化多領域整合能力。