

ISO 27001 概念解析

1. ISO 27001的全名及主要工作內容
2. 簡單說明: ISO 27001 主要分成那些領域, 控制目標/項, 及控制措施?
3. 請說明什麼是風險評估? 一般企業多久需作一次, 有那些工作/分類需進行評估呢?
4. ISMS, 與ISO 27001 的關係?

以下以**繁體中文、企業實務導向**為你完整說明 ISO 27001 與相關概念（適合資安課程或企業內訓使用）：

1 ISO 27001 的全名及主要工作內容

✓ 全名

ISO/IEC 27001

👉 Information Security Management Systems – Requirements

👉 資訊安全管理系統 (ISMS) — 要求

✓ 主要工作內容（重點精神）

ISO 27001 是一套建立、導入、維運、監控與持續改善「資訊安全管理系統 (ISMS)」的國際標準，目的在於：

- 保護企業的 **資訊資產**
- 確保資訊的：
 - **機密性 (Confidentiality)**
 - **完整性 (Integrity)**
 - **可用性 (Availability)**
- 以**風險為導向**管理資安，而非只靠技術設備

✂️ 重點不是「裝什麼設備」，而是：

制度 + 流程 + 管理 + 技術的整合

2 ISO 27001 主要分成哪些領域？

(領域 → 控制目標 / 項 → 控制措施)

(一) 整體架構概念

ISO 27001 可分為 **兩大部分**：

A 管理系統條文 (Clause 4~10)

偏向「管理制度」，例如：

條文	內容
Clause 4	組織背景
Clause 5	領導與政策
Clause 6	規劃（風險評估）
Clause 7	支援（資源、人員）
Clause 8	運作
Clause 9	績效評估
Clause 10	持續改善

👉 這部分是 建立 ISMS 的骨架

B 附錄 A（Annex A）— 資安控制措施

偏向「實際資安控管項目」

📌 依 ISO/IEC 27001:2022 版本

Annex A 共 4 大領域、93 項控制措施

領域	說明
A.5 組織控制（Organizational）	政策、風險、供應商、事件管理
A.6 人員控制（People）	人員聘用、教育訓練、離職
A.7 實體控制（Physical）	門禁、機房、設備保護
A.8 技術控制（Technological）	存取控制、加密、防火牆、惡意程式防護

🔍 控制目標 / 控制項 / 控制措施的關係

舉例說明：

- 控制目標：避免未授權人員存取系統
- 控制項：存取控制
- 控制措施：
 - 帳號密碼政策
 - 多因素驗證（MFA）
 - 權限最小化

3 什麼是風險評估？多久做一次？評估哪些項目？

✓ 什麼是風險評估 (Risk Assessment)

風險評估是 ISO 27001 的核心，目的是：

找出資訊資產可能遭受的威脅，評估風險高低，並決定如何處理

🔄 基本流程

1. 資產識別
2. 威脅識別
3. 弱點分析
4. 風險分析 (影響 × 發生機率)
5. 風險處理 (降低 / 轉移 / 接受 / 避免)

🕒 一般企業多久做一次？

時機	是否需評估
至少	每年 1 次
系統重大變更	✓
新系統上線	✓
發生重大資安事件	✓
法規或營運模式改變	✓

📁 哪些工作 / 分類需要評估？

通常包含以下類型：

類別	範例
資訊資產	資料庫、客戶資料、財務資料
IT 系統	ERP、網站、雲端系統
人員角色	系統管理員、外包人員
實體環境	機房、辦公室
第三方	雲服務商、供應商

4 ISMS 與 ISO 27001 的關係

🔗 關係說明 (一句話)

ISO 27001 是「規範」，ISMS 是「依照該規範建立的管理系統」

詳細對照

名稱	說明
ISMS	資訊安全管理系統（管理機制本身）
ISO 27001	建立 ISMS 的國際標準與驗證依據

🔗 類比：

- ISO 9001：品質管理系統（QMS）
- ISO 27001：資訊安全管理系統（ISMS）

🧠 重點快速總結

- ISO 27001 是 **以風險為核心的資安管理標準**
- 不只管技術，更管 **人、流程、制度**
- ISMS 是「系統」，ISO 27001 是「依據」
- 風險評估是整個制度的心臟 ❤️

如果你需要：

- 企業導入 ISO 27001 的流程圖
- 資安課程用簡報架構
- 與多層次防禦 / 防火牆 / IDPS 的對照說明

我可以直接幫你整理成教學版或企業實務版。

所以, ISMS 是一個系統: 資訊安全管理系統, 是以ISO 27001為核心的國際標準, 旨在協助組織建立、實施、維護及持續改進資訊安全管理。

ISO 9000是品質管理系統的標準, 與ISMS的目標不同, 互不包含。

但可互相借鑒, 對嗎? 有需補充說明的嗎?

你的理解**整體是正確的**, 而且表述得相當到位 🍊

我幫你用「**確認** → **微調** → **補充重點**」的方式整理, 讓說法在教學或考試、文件中都更嚴謹。

一、先確認你的敘述 (✓ 正確)

1 ISMS 與 ISO 27001

ISMS 是一個系統：資訊安全管理系統，是以 ISO 27001 為核心的國際標準，旨在協助組織建立、實施、維護及持續改進資訊安全管理。

✓ 正確

更精確地說是：

ISO/IEC 27001 是用來「建立與驗證 ISMS」的國際標準

ISMS 是「管理系統本身」，

ISO 27001 是「告訴你這個系統要怎麼建、怎麼管、怎麼被稽核」。

2 ISO 9000 與 ISMS 的關係

ISO 9000 是品質管理系統的標準，與 ISMS 的目標不同，互不包含。

✓ 正確

- ISO 9000（實務上指 ISO 9001）→ 品質管理（QMS）
- ISO 27001 → 資訊安全管理（ISMS）
- 兩者沒有上下位或包含關係

3 是否可互相借鑒？

但可互相借鑒

✓ 完全正確，而且是實務重點

二、建議微調成「更正式版本」的說法（可直接使用）

你原本的說法已很好，以下是企業文件／考試／簡報更常用版本：

ISMS（資訊安全管理系統）是一套以 ISO/IEC 27001 為核心依據的管理制度，用以協助組織建立、實施、維護及持續改進資訊安全管理。

ISO 9001 則為品質管理系統（QMS）的國際標準，兩者目標不同、互不包含，但在管理架構與運作方法上具有高度相似性，可相互借鑒並整合導入。

三、重要補充說明（這段很加分）

◆ 1 為什麼可以互相借鑒？

因為它們採用相同的管理系統高階架構（HLS）

ISO 管理系統共通架構（Annex SL / HLS）

項目	ISO 9001	ISO 27001
組織背景	✓	✓

項目	ISO 9001	ISO 27001
領導承諾	✓	✓
風險導向	✓ (品質風險)	✓ (資安風險)
文件化	✓	✓
內部稽核	✓	✓
持續改善 (PDCA)	✓	✓

🔴 差別在於：

- 管什麼不同
- 管理的方法與精神相同

◆ 2 風險導向是兩者的「共通核心」

標準	風險內容
ISO 9001	品質風險、流程失效
ISO 27001	資訊安全風險 (CIA)

👉 所以：

- 做過 ISO 9001 的企業
- 導入 ISO 27001 會快很多

◆ 3 實務上常見「整合式管理系統」

很多企業會：

- **ISO 9001 + ISO 27001**
- 共用：
 - 文件管制程序
 - 內稽內控
 - 管理審查
 - 教育訓練
- 只在「專業控管項目」分開 (品質 vs 資安)

🔴 稽核時：

- 一套制度
- 多張證書

四、可補充的一句「總結金句」（很適合考試或簡報）

ISO 9001 與 ISO 27001 雖屬不同管理目標，但同樣基於 PDCA 與風險導向思維，能有效整合運作，提升組織整體治理與管理成熟度。

如果你願意，我也可以幫你整理成：

- 📌 一張對照表（ISO 9001 vs ISO 27001）
- 📌 考試用精簡版答案
- 📌 企業導入整合 ISMS + QMS 的流程圖

你比較想用在哪一種情境？

ISO 的全名？

ISO 的全名是：

International Organization for Standardization

👉 國際標準化組織

📌 補充重點（常考／易混淆）

- ISO 不是「International Standards Organization」（這是很多人會誤寫的 ❌）
- ISO 這個縮寫不是從英文或法文直譯，而是來自希臘文「isos」
👉 意思是「相同、一致」

🧠 一句記憶版

ISO = International Organization for Standardization（國際標準化組織）

如果你需要「考試版一行答案」或「搭配 ISO 9001 / 27001 的完整介紹」，我可以再幫你整理。

上面提及: Annex A 共 4 大領域、93 項控制措施
為何沒提到控制項？
控制項的角色是什麼？

這個問題問得非常好，而且很關鍵 🙌

其實你已經碰到 ISO 27001:2022 改版後，最多人混淆的觀念之一。

我分成「為何沒提控制項」→「控制項是什麼」→「它現在扮演的角色」三個層次來說明。

一、為何在 Annex A 只說「93 項控制措施」，而沒再提「控制項」？

🔑 關鍵原因：名詞角色改變了

在 ISO/IEC 27001:2022 版本中：

- 「控制項 (Control Objective)」被弱化甚至不再單獨列出
- Annex A 直接以「控制措施 (Controls)」為主體

👉 也就是說：

控制項的功能，已被「具體控制措施本身」所吸收

⬅️ 舊版 (ISO 27001:2013) 的結構

以前是三層結構：

markdown

控制領域

└ 控制目標 (Control Objective)

└ 控制措施 (Controls)

例如：

- 控制目標：確保資訊存取的適當性
- 控制措施：
 - 使用者存取管理
 - 特權帳號管理

↔️ 新版 (ISO 27001:2022) 的結構

現在變成 兩層結構：

控制領域

└ 控制措施 (Controls)

🔑 不再強制列出「控制目標」

二、那「控制項」到底是什麼？（角色說明）

✅ 控制項 (Control Objective) 的本質

控制項不是技術，而是：

「為什麼要做這些控制」的管理目的

也就是：

- 要達成什麼安全狀態
- 要避免什麼風險

🔍 舉例說明（用舊觀念幫助理解）

名稱	說明
控制項（目標）	防止未授權存取
控制措施	密碼政策、MFA、權限最小化

- 👉 控制項是「目的」
- 👉 控制措施是「方法」

三、在 2022 版中，控制項的角色變成什麼？

◆ 1 控制項「內化」到風險評估與 SoA 中

在新版 ISO 27001：

- 風險評估 → 決定「要不要這個控制」
- 風險處理計畫
- SoA（適用性聲明）

👉 控制項的「目標性」是由企業自己定義，而不是標準強制給你

◆ 2 Annex A 控制措施已自帶「目的描述」

每一項控制措施都有：

- **Control**：控制措施說明
- **Purpose**：這項控制想達成什麼

👉 **Purpose** 就是「隱含的控制項」

◆ 3 管理彈性更高（這是改版的重點）

新版精神是：

控制措施 ≠ 必須全部做
而是依風險選擇最適合的控制

所以：

- 不再用固定的控制項綁死
- 鼓勵風險導向與情境導向

四、控制項現在的「實務角色」是什麼？

 在企業實務中，控制項仍然存在，只是：




場景	控制項的角色
風險評估	作為風險對應的「安全目標」
SoA 撰寫	說明「為何採用 / 不採用」
內部稽核	判斷控制是否達成目的
教學 / 溝通	幫助理解控制措施的意義

 只是它不再是 Annex A 的正式層級名稱

五、一句話總結（這句很重要）

ISO 27001:2022 並不是「沒有控制項」，而是「不再把控制項當成獨立清單列出」，而是將其目的直接融入各項控制措施與風險管理流程中。

如果你願意，我可以：

-  幫你做一張 **2013 vs 2022 控制項結構對照表**
-  用 **考試答題版** 幫你整理一句標準答案
-  從 **企業導入 ISMS 文件角度**，說明控制項如何實際寫進文件

你比較想要哪一個？