歐盟網路韌性法案 (CRA) 常見問題集

《網路韌性法案》(歐盟法規 Regulation (EU) 2024/2847) 針對投放到歐盟市場且具備數位元件之產品，導入了強制性的網路安全要求。

1. 什麼是歐盟《網路韌性法案》？

《網路韌性法案》(歐盟法規 Regulation (EU) 2024/2847) 針對投放到歐盟市場且具備數位元件之產品，導入了強制性的網路安全要求，適用於硬體與軟體。

CRA 要求製造商在產品的整個生命週期中，必須確保其設計、開發與維護之安全性，包括「安全納入設計」的開發模式、漏洞管理、資安事件通報及技術文件的編製。

如果您將連網產品或軟體投放到歐盟市場銷售，這項法規很可能適用於您。

2. CRA 何時開始適用？

CRA 已於 2024 年 12 月正式生效。然而，相關法規義務將分階段逐步實施：

- 2026 年 9 月 11 日：強制通報義務正式實施，製造商必須通報已遭利用的漏洞與重大資安事件。
- 2027 年 12 月 11 日：全面強制實施網路安全要求與 CE 標誌之法定義務。

自 2026 年 9 月起，通報義務亦適用於已在歐盟市場銷售的既有產品。製造商必須在 2026 年 9 月之前採取行動，以避免出現合規漏洞。另請參閱下文第 8 項。

3. CRA 是否適用於歐盟境外企業？

是的。不論企業位於何處，任何將具備數位元件之產品投放到歐盟市場的製造商，都必須遵守 CRA。非歐盟境內的製造商必須確保符合 CRA 規範，並可指定一名「歐盟授權代表」。此外，歐盟境內的進口商與經銷商在 CRA 法規下亦負有法律義務。

4. 哪些產品屬於 CRA 的管制範圍？

CRA 適用於所有具備數位元件的產品，意指其預期用途或可合理預見的用途涉及與設備或網路建立直接或間接的邏輯或實體資料連接。

5. 什麼是「具備數位元件的產品」？

凡是預期用途或可合理預見的用途，包含對設備或網路建立直接或間接資料連接的任何硬體或軟體，皆屬於具備數位元件的產品。產品包含：

- 物聯網與智慧裝置
- 消費性電子產品
- 工業控制系統
- 網路設備
- 獨立軟體
- 行動應用程式
- 韌體與嵌入式系統
- 硬體元件（如處理器或安全晶片）

若雲端或遠端資料處理服務是產品功能所必需，則亦可能被納入管制範圍。

6. 獨立軟體與行動應用程式是否涵蓋在內？

是的。CRA 明確將投放到歐盟市場的獨立軟體納入管制，包含：

- 桌上型應用程式
- 作業系統
- 韌體
- 行動應用程式
- 開發工具
- 商業化程式庫與軟體開發套件

7. 製造商的主要義務是什麼？

製造商必須履行以下事項：

- 執行並記錄網路安全風險評估
- 依據基本網路安全要求設計產品
- 落實安全開發實踐
- 在產品支援期間內提供安全更新，通常至少為五年，且須與產品的預期壽命保持一致
- 建立漏洞處理流程
- 在嚴格的法定期限內，通報已遭利用的漏洞與重大資安事件
- 編製技術文件

©Intertek - All rights reserved. EL-CRAFAQ-V1-0726TC

這並非一次性的措施；CRA 引入的是貫穿整個產品生命週期的持續性義務。

8. 漏洞與資安事件的通報要求為何？

自 2026 年 9 月 11 日起，製造商必須通報：

- 已遭利用的漏洞
- 影響具備數位元件產品的重大資安事件

製造商必須提交：

- 在得知已遭利用的漏洞或重大資安事件後 24 小時內發出預警
- 在 72 小時內提交詳細通知
- 根據需要提供後續追蹤資訊與補救措施更新

所有報告須透過歐盟網路安全局 (ENISA) 管理的歐盟通報平台進行提交。

自 2026 年 9 月起，通報義務適用於仍在支援期間、且受 CRA 規範的產品，包括在 CRA 主要合規日期之前已在歐盟上市的產品。

9. 什麼是「重要產品」與「關鍵產品」？

CRA 依據風險高低將產品分為以下類別：

- 預設類別 (一般產品)：絕大多數的連網產品皆屬於此類，通常允許進行自我評估。
- 重要類別 I：包含作業系統、瀏覽器、路由器、密碼管理器，以及智慧家庭安全設備等產品。
- 重要類別 II：包含風險較高的基礎設施元件，如防火牆、入侵偵測/防禦系統和虛擬化管理程序。
- 關鍵產品：包括硬體安全模組、智慧卡、安全元件，以及特定安全敏感設備。

重要類別 II 產品需經由公告機構進行第三方符合性評估。關鍵產品則需通過歐洲網路安全認證；若沒有適用的認證方案，則需透過公告機構進行符合性評估。

10. 我需要透過公告機構進行驗證嗎？

這取決於產品的類別。多數一般產品可以採用自我評估方式，或適用調和標準 (重要類別 I 產品)。

重要類別 II 產品需要由公告機構進行第三方符合性評估。關鍵產品則需通過歐洲網路安全認證；若沒有適用的認證方案，則需透過公告機構進行符合性評估。

提早確認產品分類至關重要，以免耽誤產品上市時程。

11. 需要準備哪些技術文件？

製造商必須編製並維護技術文件，以證明符合歐盟法規 Regulation（EU）2024/2847。至少包括：

- 網路安全風險評估 (涵蓋已識別風險、緩解措施與殘餘風險)
- 證明符合 Annex I 基本網路安全要求的技術文件
- 產品說明及其預期用途，包含架構與相關元件
- 安全開發與生命週期流程（包含配置與更新機制）
- 漏洞處理流程，包含協調漏洞揭露程序
- 軟體物料清單 (SBOM)
- 使用手冊與資訊，包含安全設定、支援期間與更新資訊
- 歐盟符合性聲明
- 符合性評估文件，在適用情況下，需包含公告機構核發的證書

技術文件必須保持最新狀態，以反映產品修改、安全更新以及新識別的風險。

For more information

台北 +886 2 66022888 #729
台中 +886 4 23598819 #814
website.tw@intertek.com

www.intertek-twn.com

©Intertek - All rights reserved. EL-CRAFAQ-V1-0726TC