歐盟網路韌性法案
Cyber Resilience Act (CRA)

歐盟對具備數位元件產品的網路安全要求

Intertek 為製造商提供完整的《網路韌性法案》符合性支援服務，涵蓋從產品分類、符合性差距分析、安全測試與驗證、技術文件建置，到最終符合性評估等全流程工作，協助企業符合 CRA 法規要求。

什麼是歐盟《網路韌性法案》？

《網路韌性法案》(Cyber Resilience Act, CRA, EU 2024/2847) 針對投放歐盟市場且具備數位元件之產品，導入強制性的網路安全要求。

該法規涵蓋硬體、軟體及嵌入式韌體，並適用於產品的整個生命週期，包含設計與開發階段，以及漏洞管理與資安事件通報等。

根據《網路韌性法案》，對於投放歐盟市場且具備數位元件之產品而言，符合網路安全要求將成為取得 CE 標誌的必要條件之一。

《網路韌性法案》將於 2027 年 12 月 11 日全面實施，屆時，所有具備數位元件之產品均須符合 CRA 規定的網路安全要求，方可在歐盟市場合法上市。

誰需要符合規範？

凡將具備數位元件之產品投放至歐盟市場的製造商、進口商及經銷商，均有義務遵守《網路韌性法案》的相關規定。

CRA 適用範圍

《網路韌性法案》適用於具備數位元件之產品，亦即能夠直接或間接連接至其他裝置或網路的硬體或軟體產品。適用範圍包括：

- 連網硬體設備
- 軟體產品
- 嵌入式軟體或韌體
- 需透過雲端或遠端服務才能正常運作的產品
- 工業用及消費性連網產品

與《無線電設備指令》(RED) 授權法案中的網路安全要求所涵蓋的產品不同，CRA 不僅適用無線電設備，更廣泛適用於任何能夠直接或間接連接至網路或其他裝置的產品。

關鍵日期

- CRA 正式生效： 2024 年 12 月 10 日
- 事件通報義務： 2026 年 9 月 11 日
- CRA 全面實施： 2027 年 12 月 11 日

CRA 規範的產品類別

《網路韌性法案》依風險等級對產品進行分類，並據此類別決定其符合性評估要求。

重要類別 I (Annex III)

資安漏洞可能影響資料機密性、完整性或可用性的產品，例如：

- 作業系統
- 密碼管理工具
- 網路管理工具
- 瀏覽器
- 遠端存取軟體
- IoT 管理平台

符合性評估路徑：採用調和標準進行自我評估。

重要類別 II (Annex III)

若發生故障，可能會中斷關鍵功能或服務的產品，例如：

- 防火牆
- 入侵偵測/防禦系統
- 虛擬化管理程式
- 安全元件

符合性評估路徑：必須由公告機構進行符合性評估。

關鍵產品 (Annex IV)

被視為建立信任基礎或提供關鍵服務的產品，例如：

- 具備安全模組的硬體設備
- 智慧電表系統中的智慧電表閘道器
- 智慧卡或類似裝置

符合性評估路徑：須通過歐洲網路安全認

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

歐盟網路韌性法案
Cyber Resilience Act (CRA)

證體系；若無適用的認證體系，則須經由公告機構進行評估。

預設類別

指未被列入 Annex III 或 Annex IV 的數位元件產品，例如：

- 消費性物聯網設備
- 應用軟體
- 智慧家庭設備
- 許多工業用聯網設備

符合性評估路徑：自我評估。

CRA 網路安全需求《Annex I》

採用風險導向方法，製造商必須確保產品符合以下網路安全要求：

- 安全設計與預設安全
- 依循安全開發流程與實務進行開發
- 在交付時已解決已知漏洞
- 提供必要的安全更新
- 防止未經授權的存取
- 將攻擊面降至最低
- 防範資料竄改與外洩
- 具備記錄與監控資安事件的能力
- 提供清楚且完整的安全技術文件

製造商亦須履行以下義務：

- 進行網路安全風險評估
- 維護軟體物料清單
- 建立並執行漏洞管理流程
- 通報已遭利用的漏洞與資安事件
- 在產品支援期間提供安全更新與修補程式

CRA 符合性評估流程

製造商若要將具有數位元件的產品投放至歐盟市場，必須遵循 CRA 的符合性評估流程：

1. 進行產品分類 (預設類別、重要類別 I、重要類別 II、關鍵類別)。
2. 落實 CRA 網路安全要求 (安全開發、風險評估、漏洞處理)。
3. 編製完整技術文件，以證明符合 CRA《Annex I》之規範。
4. 完成符合性評估 (依產品分類進行自我評估或由歐盟公告機構驗證)。
5. 簽發歐盟符合性聲明，此為取得 CE 標誌的必要文件。
6. 履行上市後網路安全義務，包含漏洞處理與資安事件通報。

技術文件必須包含以下內容：

- 產品說明
- 系統架構與設計資訊
- 風險評估報告
- 軟體物料清單
- 安全更新政策
- 漏洞處理政策
- 資安事件通報程序
- 對應 CRA《Annex I》之要求
- 測試報告與相關證明

CRA 準備工作

製造商現應立即著手進行以下準備工作：

- 確認產品類別
- 進行 CRA 差距分析
- 執行網路安全風險評估
- 導入安全開發生命週期流程
- 編製技術文件
- 規劃符合性評估與 CE 標誌

網路安全測試與認證服務

除了提供《網路韌性法案》的合規支援服務外，Intertek 還針對聯網產品與軟體提供廣泛的網路安全測試、認證和諮詢服務，以協助您符合全球市場的法規要求、滿足客戶需求，並確保產品的安全開發。

Intertek 依據以下國際標準與法規為製造商提供網路安全測試與認證服務：

- IEC 62443：工業網路安全標準
- EN 18031：符合歐盟無線電設備指令 (RED) 授權法案的網路安全要求
- ETSI EN 303 645：消費性物聯網的網路安全標準
- IEC 81001-5-1：醫療器材安全軟體生命週期流程標準
- 漏洞評估與滲透測試
- 安全架構審查與威脅建模
- 加密模組評估 (FIPS 140-3)
- 共同準則
- AI 紅隊演練
- 勒索軟體韌性評估

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-CRA-V1-0726TC