# 為符合歐盟《網路韌性法案》(CRA) 第 14 條做好準備

卷 8 | 期數 32 | 2026 年 6 月
作者： Karl Lau, Tommy Leung; 校對：Joey Kwok

## 重點摘錄


- 歐盟《網路韌性法案》(CRA)，即 (EU) 2024/2847 號條例，對進入歐盟市場的數位產品提出了迄今為止最嚴格、最全面的網路安全要求。其中，第 14 條——強制性漏洞和事件報告——將於 2026 年 9 月 11 日生效，這意味著製造商只有有限的時間來實施合規流程。
- 本白皮書概述了法案框架，重點介紹了第 14 條帶來的關鍵合規挑戰，並介紹了 CMA 檢定中心 的自動化合規解決方案。該解決方案旨在幫助企業有效率、準確、大規模地履行報告義務。

# 1. 歐盟網路韌性法案 (CRA) 概述

《網路韌性法案》(CRA)是歐盟首部涵蓋**所有含數位元素產品**的橫向網路安全法規。其基礎是一項統一原則：

**「安全設計」與生命週期網路安全保障結合**

## 關鍵監管目標

- **安全設計產品：**上市時不存在已知可利用漏洞
- **預設安全性配置**
- **強制性漏洞管理和免費安全性更新**
- **全生命週期網路安全責任**
- **統一的歐盟合規要求，消除分散的國家法規**

## 覆蓋範圍

- 硬體產品
- 軟體應用
- 相關遠端資料處理服務（例如，雲端連接的智慧家庭系統）

# 2. 產品範圍和風險分類

法案將產品分為三種風險等級，幾乎涵蓋所有數位產品：

## 2.1 通用數位產品

所有連網或具備數位化功能的產品，包括：

- 消費性電子產品
- 辦公室軟體
- 智慧家電

## 2.2 重要產品（強制性第三方評估）

### 一級（中度風險）

- 營運系統
- 路由器
- 智慧門鎖
- 密碼管理器
- 智慧攝影機
- 穿戴式健康設備
- 智能玩具

### 類別 II（高風險）

- 防火牆
- 入侵偵測/防禦系統
- 虛擬機器管理程序
- 容器運作時系統
- 防篡改處理器和微控制器

## 2.3 關鍵產品

- 硬體安全模組 (HSM)
- 安全元件和晶片
- 智慧卡
- 智慧電錶網關
- 進階加密設備

這些產品需要根據**歐盟統一框架獲得 EUCC 認證**。

## 3. 承擔責任的相關經濟體

法案對整個供應鏈施加了義務及責任：

| 持份者 | 責任 |
| --- | --- |
| **生產商** | 設計、測試、漏洞管理、安全性更新、生命週期合規性 |
| **進口商** | 驗證 CE 標誌和合規性文件 |
| **分包商** | 確保銷售合規產品；報告風險 |
| **自有品牌/修改器** | 承擔全部製造商責任 |
| **開源維護者** | 有限義務（僅適用於商業化的開源產品） |

## 4. 不合規的後果

- **罰款：最高可達全球年營業額的 2.5% 或 1,500 萬歐元（以較高者為準）**
- **市場執法措施：**
  - 產品禁令
  - 強制召回
  - 退出歐盟市場
- **其他後果：**
  - 沒收非法所得
  - 市場准入限制
  - 消費者集體訴訟

# 5. 關鍵實施時間表

| 日期 | 里程碑 | 緊急程度 | 所需操作 |
|---|---|---|---|
| 2026 年 9 月 11 日 | 第 14 條強制報告生效 | ⭐ ⭐ ⭐ ⭐ ⭐ | 部署事件回應和自動化報告系統 |
| 2027 年 12 月 11 日 | 全面執行《消費者報告法》（強制要求 CE 標誌） | ⭐ ⭐ ⭐ | 完成所有產品的合規性認證 |

# 6. 第十四條：核心合規挑戰

## 6.1 強制報告觸發因素

製造商在以下情況必須報告:

- **已發現被主動利用的漏洞**
  - 現實世界攻擊或概念驗證（PoC）流傳的證據
- **• 發生嚴重的安全事件**，例如：
  - 惡意程式碼注入
  - 大規模資料外洩
  - 設備故障

## 6.2 嚴格的報告截止日期

| 截止日期 | 要求 |
|---|---|
| 24 小時內 | 早期預警通知（發送給國家網路安全事件回應小組和歐盟網路安全局） |
| 72 小時內 | 詳細事件報告（影響、範圍、緩解措施） |
| 14 天/1 個月內 | 最終報告（補救後報告或事件結論） |

這些時間節點**為營運帶來了極大的壓力**，尤其對於需要管理以下事項的全球分散式團隊：

- 時區差異
- 週末突發事件
- 語言和監管報告要求

即使是輕微的延誤或錯誤也可能導致**監管處罰或市場退出**。

# 7. CMA 檢定中心：端到端第 14 條合規解決方案

CMA 檢定中心 提供**完全符合規範的自動化漏洞報告雲端服務**，旨在解決第 14 條規定的操作和技術挑戰。

## 7.1 SBOM 自動化和管理

- 自動產生或匯入**軟體物料清單 (SBOM)**
- • 與全球漏洞資料庫即時連接
- **10 分鐘**內完成所有組件的完整影響分析

## 7.2 透過 VEX 進行智慧過濾

- 整合**漏洞利用交換平台 (VEX)**
- 自動過濾 **60% 以上的誤報**
- 在維持合規準確性的同時，減少報告工作量

## 7.3 人工智慧驅動的報告自動化

- 階段自動產生符合 ENISA 標準的英文報告：
  - 預警報告
  - 詳細報告
  - 最終報告
- 一鍵人工驗證，然後直接提交至 ENISA 平台
- 旨在可靠地滿足 24 小時/72 小時的截止日期要求

### 7.4 端到端可視性和協調揭露

- 即時儀錶板，用於：
  - 合規期限
  - 報告狀態
- • 整合**協調漏洞揭露（CVD）**入口網站：
  - 統一的內部和外部報告入口

### 7.5 隨時可進行審計的合規性和全天候監控

- 完整的**活動日誌記錄**，確保符合法規要求
- 自動化合規記錄歸檔
- **全天候監控和警報**，確保零報告漏洞

## 8. 額外的合規要求

除了第 14 條之外，各組織還必須履行持續義務：

- ✅ **至少 5 年免費安全更新**（工業產品更新時間更長）
- ✅ 強制性 **SBOM 生成和維護**
- ✅ 安全性更新要求：
  - 預設自動更新（消費性產品）
  - 所有產品均提供退出機制
- ✅ 清晰的**支援生命週期披露**和用戶通知
- ✅ 違規行為可能面臨消費者集體訴訟

# 9. 結論：必須立即採取行動

CRA 第 14 條規定了**零過渡、零豁免**的要求。所有已在歐盟市場銷售的數位產品必須在 **2026 年 9 月 11 日**前符合規定。

未能建立合規機制的組織：

- 事件回應機制
- 自動漏洞報告
- 生命週期安全流程

**將面臨重大的財務、營運和聲譽風險**，包括市場排斥。