

CRA導入評估說明

Regulation (EU) 2024/2847
Cyber Resilience Act
歐盟《網路韌性法》

rongchi_liao

2026 / 11 / 02

DIVA Labs.

歐盟公告網路韌性法(Cyber Resilience Act)

歐盟執委會於2024年11月20日以REGULATION (EU) 2024/2847公告旨揭法案文本，依據歐盟執委會官方網頁，該法案係歐盟首個針對數位軟硬體產品，引入網路安全規範之水平式立法，未來相關產品上市時，須遵守統一規範。

此外，該法將針對產品設計、開發及維護等產品生命週期各階段，建立網路安全要求框架及產品製造商、進口商、經銷商應履行之義務，旨揭法規生效後，具聯網功能之數位軟硬體產品需有CE標章以示符合法規規定，以提升產品網路安全性。(排除開源碼軟體或醫療設備、航空汽車等已受現有法規規範之產品)

DIVA Labs.

申請／導入原因

CRA Cyber Resilience Act歐盟《網路韌性法》已進入執行階段，DIVA需提前建立可稽核的產品資安治理機制

Regulation (EU) 2024/2847適用範圍

含數位元素的產品納入管理
其中Monitor亦屬評估範圍

2026.09.11

漏洞管理與嚴重資安事件通報義務開始適用

2027.12.11

主要產品符合性要求全面適用

未提前建置的主要風險

法規	需提出風險評估、SBOM、漏洞處理與符合性證據,以符合標準EU 2024/2847
市場	2027年底標準生效後出口歐盟產品,必須強制符合性CRA聲明以符合**CE**要求
財務	章節中Article 64說明,不符合者,將予以處以最高罰款可達1,500萬歐元或全球年營業額2.5%

CE

DIVA Labs.

Qisda集團作法

集團提供方向與窗口，各事業單位仍需自行建立制度並選擇輔導機構

集團目前作法

01 BenQ與Qisda,以各自成立PSIRT產品資安事件應變團隊，並與R&D配合

02 PM／RD／QA為產品資安事件的主要責任窗口

03 資安、客服、測試等單位依案件協作

04 設計驗證團隊負責產品測試及CRA符合性認證

05 目前沒有集團統一的CRA輔導或教育訓練

外部輔導原則

集團立場	沒有指定或推薦廠商，可自行選擇或由客戶指定，無評估集團教育訓練計畫
可接洽集團機構	TÜV、UL Solutions、Auray、TÜV SÜD、SGS
建置模式	各機構作法大致相近，差異主要在費用與服務範圍
導入方式	首次開案後，由選定機構提供完整輔導

結論：DIVA需自行選擇LAB並建立CRA架構

DIVA Labs.

培訓主題與建議參與部門

PSIRT應變團隊應由產品資安、研發、產品管理、法規及品質共同參與

培訓主題	主要內容	主責單位	主要參與	建議參與
Risk Assessment 風險評估	產品範圍、威脅情境、風險判定及控制措施	PSIRT應變團隊／PM／R&D	跨部門PSIRT 、產品管理部、韌體課、軟體課、設計驗證工程課、必要時加入硬體課、機構課	資訊課、採購課、品保部
Vulnerability Handling漏洞處理	SBOM、漏洞監控、事件分級、修補及法規通報	PSIRT應變團隊	跨部門PSIRT 、產品管理部、韌體課、軟體課、採購課、品保部	設計驗證工程課、資訊課
SecureDevelopment Lifecycle (SDLC) 產品安全開發生命週期	安全需求、設計審查、驗證、版本與生命週期管理	PSIRT應變團隊／R&D／QA	跨部門PSIRT 、產品管理部、韌體課、軟體課、品保部	設計驗證工程課、資訊課、採購課

建議窗口：PM/R&D/QA擔任產品主要負責單位，其他各部門指派固定窗口參與後續制度建置。

DIVA Labs.

DIVA評估事項

採兩階段導入，可先完成通報與漏洞治理基礎，再銜接最終產品合規

2026.11 啟動 — 1 — **2027.01 完成第一階段** — 2 — 3 — **2027.12.11 前完成**

第一階段｜Item 1～3　NTD 550,000

預估期間：2～3個月,是否由TÜV SÜD執行第一階段

- ✓ Item 1 產品資安風險評估
- ✓ Item 2 SBOM與供應鏈元件盤點
- ✓ Item 3 漏洞管理、通報及PSIRT基礎機制

第二階段｜Item 4～5　待標準明確後執行

建議2027 Q1～Q2確認要求後啟動

Item 4	**產品測試認證** 單一型號 NTD 50,000
Item 5	**產品生命週期管理** NTD 250,000

DIVA Labs.



THANK YOU