# 歐盟《Cyber Resilience Act (CRA)》合規白皮書

## ASRock Industrial Cyber Resilience Act (CRA) Compliance White Paper

發佈單位：東擎科技股份有限公司 (ASRock Industrial Computer Corp.)
發佈日期：2026 年 7 月
更新日期：2026 年 9 月 2 日

### 1. 前言與摘要 (Executive Summary)

東擎科技 (ASRock Industrial) 致力於提供安全、可信賴的邊緣 AI 運算平台，並協助全球客戶建置符合國際資安標準及法規要求的產品與解決方案。

為持續提升產品資安能力與供應鏈信任，東擎科技已建構完整的資訊安全治理制度，並取得多項國際資安標準認證，包括：

- ISO/IEC 27001:2022 (資訊安全管理系統認證)
  Certificate No. 2026/117844.1
- IEC 62443-4-1 (安全產品開發生命週期認證)
  Certificate No. NL-103556
- IEC 62443-4-2 (工業控制元件技術安全認證)
  Certificate No. NL-113417
- FIDO Device Onboard (FDO 安全裝置上線認證)
  Certificate No. FDO000020240906004

本白皮書說明東擎科技針對歐盟《Cyber Resilience Act（CRA）》所建立之產品安全架構、合規策略及持續維運機制，協助客戶因應歐盟市場之資安法規要求。

### 2. 關於歐盟《Cyber Resilience Act》（CRA）

《Cyber Resilience Act（CRA）》係歐盟針對具備數位元素之產品（Products with Digital Elements, PDE）所制定之強制性網路安全法規，要求製造商於產品設計、開發、生產及產品支援期間落實基本網路安全要求，建立漏洞管理、安全更新及事件通報機制，以提升產品整體網路安全韌性。

東擎科技依循 CRA 法規要求，將資訊安全納入產品生命週期各階段，並持續推動產品安全治理，其核心實踐包括：

- **資安內建（Security by Design）**：東擎科技於產品設計與開發階段即導入資安要求，透過風險分析、威脅建模及安全設計機制，將資訊安全納入產品開發流程。



Storage Retention: 2 Years

The information contained herein is the exclusive property of ASRock Industrial and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of ASRock Industrial.

- **產品支援期間之資安管理**：東擎科技於產品支援期間持續提供資安維護、安全更新及漏洞修補，以維持產品之網路安全能力。
- **漏洞處理與事件通報**：自 2026 年 9 月 11 日起，東擎科技依循 CRA 規定，針對遭主動利用之漏洞（Actively Exploited Vulnerabilities）及重大資安事件（Severe Incidents）履行法定通報義務，並採取必要之修補與風險降低措施。

## 3. 產品適用範圍

本白皮書適用於東擎科技提供之具備數位元素產品，包括：

- 工業電腦主機板 (Industrial & Embedded Motherboards)
- 嵌入式工業電腦系統 (Embedded Computer Systems)
- 工業級強固邊緣 AIoT 系統平台 (Industrial Robust Edge AIoT Platform)

東擎科技依據 CRA 要求及產品風險分類，持續進行產品安全設計、合規審查及資安維運管理。

## 4. CRA 深度防禦與合規策略

東擎科技採取「Secure by design」架構，從開發流程、產品設計到後續維運，全面對接 CRA 規範：

### 4.1 安全開發流程 (Secure Development Lifecycle)

東擎科技之安全開發流程已通過 IEC 62443-4-1 認證，並持續依循 CRA 要求及相關國際標準 prEN 40000 系列之要求，建立完善之安全產品開發流程並落實以下機制：

- 風險分析與威脅建模 (Risk assessment &Threat Modeling)：在產品設計初期執行資安風險分析與威脅建模，識別潛在攻擊情境，並將風險納入產品設計與控制措施。
- 程式碼安全審查與測試：結合靜態與動態資安測試 (SAST/DAST)，於開發過程中持續驗證程式碼安全性。
- 軟體物料清單 (SBOM)：建立並維護 SBOM(SPDX/CycloneDX)，支援漏洞管理與供應鏈透明化要求。

### 4.2 產品資安硬體設計

東擎科技將資安能力內建於硬體、韌體及平台架構，依據各產品之資安風險評估結果，提供支援符合 CRA Annex I《Essential Cybersecurity Requirements》之安全功能。主要安全機制包括：

- 硬體信任根 (Hardware Root of Trust)：整合 TPM 2.0 提供硬體層級的金鑰保護與開機完整性量測，並搭配 UEFI Secure Boot 逐級驗證開機鏈，確保裝置僅執行經簽章授權的韌體與系統程式，為資料機密性與系統完整性提供硬體級保障。
- 可信賴的安全更新：支援韌體及系統更新映像之簽章驗證，確保安全性更新可於支援期間內持續、可靠地送達裝置。
- 攻擊面最小化與安全預設：產品以安全預設（Secure by Default）組態出貨，未使用之實體介面與除錯埠預設關閉或受控管理，並支援回復原廠安全設定，降低產品於支援期間內之攻擊面。

### 4.3 漏洞管理與 PSIRT 機制

東擎科技已成立 產品資安事件應變小組 Product Security Incident Response Team（PSIRT），建立完整



Storage Retention: 2 Years

The information contained herein is the exclusive property of ASRock Industrial and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of ASRock Industrial.

之產品漏洞管理制度，包含：

- 協同漏洞揭露 (CVD)：保持透明溝通，即時修補已知漏洞。
- 時效性修補：於支援期間內即時(without undue delay)提供安全性更新。

更多資訊請參閱東擎 Security Center https://www.asrockind.com/security-center

**5. CRA 合規推動時程 (Roadmap)**

東擎科技持續依 CRA 要求推動產品資安治理，並規劃以下合規推動時程：

| 階段 | 預定時程 | 合規執行說明 |
|---|---|---|
| 第一階段 | 已完成 | 取得 IEC 62443-4-1 / 4-2 認證，東擎科技已具備安全產品開發及產品安全能力。 |
| 第二階段 | 已完成 | 取得 ISO/IEC 27001:2022 認證，強化企業資訊安全治理與 SBOM 管理流程。 |
| 第三階段 | 已完成 | 建立符合 CRA 要求之漏洞通報制度，全面啟動 PSIRT 與漏洞管理流程，以因應 2026 年 9 月起適用之漏洞通報規定。 |
| 第四階段 | 2027 起<br>(持續維運) | 建立輸歐產品持續性資安維運機制，依 CRA 要求執行漏洞管理、安全更新及產品安全監控，確保產品於支援期間持續符合相關網路安全要求。 |

**6. 法律聲明與聯絡資訊**

本白皮書所載之技術架構、合規策略、規劃時程及未來目標，僅供資訊參考，不構成任何法律、商業或契約保證。產品之功能規格、SBOM 提供方式、資安更新政策及售後支援服務，均以雙方正式簽署之契約、產品規格書及官方技術文件為準。

如需了解更多關於歐盟 CRA 法規或東擎資安方案，請與東擎聯繫：

- 官方網站：ASRock Industrial Official Website
- 產品與合規諮詢：Product Inquiry



Storage Retention: 2 Years

The information contained herein is the exclusive property of ASRock Industrial and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of ASRock Industrial.