CRA EVIDENCE 白皮書

EU 網路韌性法案：實務合規指南

本白皮書提供給數位元素產品的製造商、進口商與經銷商參考。

編製	CRA Evidence
版本	1.0
狀態	動態文件
依據	EU 規則 2024/2847

變更紀錄

本文件為動態文件，將隨歐盟指引、調和標準與市場實務的演進而更新。

版本	日期	說明
1.0	2026年5月17日	初次公開發布。涵蓋適用範圍、分類、實質修改、必要要求、漏洞處理、技術檔案、符合性評鑑路徑，以及與 AI Act、Data Act、ESPR 與產品責任的關係。

目錄

摘要

60 秒重點

涵蓋範圍： 在 EU 市場供應的連網硬體與軟體產品。資安改為以產品合規要求處理，而非僅是最佳實務。

適用時點： 第 14 條通報義務自 2026 年 9 月 11 日開始；完整技術、文件與 CE 標章義務自 2027 年 12 月 11 日開始。

必須產出的資料： 資安風險評估、SBOM、技術檔案、使用者說明、EU 符合性聲明、CE 標章，以及第 14 條事件與漏洞通報。

誰需要行動

製造商承擔主要責任。進口商與經銷商在供應產品前，需要執行注意義務檢查。

改變是什麼

資安成為產品合規的一部分：安全設計、漏洞處理、文件、CE 標章與上市後行動。

第一個期限

第 14 條通報於 **2026 年 9 月 11 日**開始，適用於遭主動利用的漏洞與嚴重事件。

完整適用

完整技術合規自 **2027 年 12 月 11 日**適用。既有產品在實質修改後納入，但通報義務仍適用。

證據核心

技術檔案需要風險評估、SBOM、支援期間依據、測試證據、使用者說明、聲明，以及符合基本資安要求的證據。

符合性路徑

多數產品可使用模組 A 自我評鑑。重要與關鍵產品可能需要公告機構，或採用 EU 資安認證路徑。

CRA 將資安變成產品要求

EU 規則 2024/2847，也就是網路韌性法案（CRA），是 EU 第一個將資安列為數位元素產品強制要求的橫向框架。正式文本可在 EUR-Lex 查閱。

CRA 適用於連網硬體與軟體的製造商、進口商與經銷商。範圍涵蓋從消費性 IoT 裝置到工業控制系統。實務上的改變很直接：資安必須成為產品合規的一部分，並且需要設計、留存證據、維護與監控。

違反基本資安要求或第 13 條與第 14 條義務，可能導致最高 1,500 萬歐元，或全球年度營業額 2.5%（取較高者）的罰鍰。也適用較低層級：違反其他指定義務最高 1,000 萬歐元或 2%，向公告機構或市場監督機關提供不正確、不完整或誤導性資訊最高 500 萬歐元或 1%。市場監督機關也可以要求矯正措施、限制供應、撤回產品，或要求召回。

合規規劃的關鍵日期

CRA 已於 **2024 年 12 月 10 日**生效。實務合規工作可按三個節點推進：**2026 年 6 月**的公告機構規範、**2026 年 9 月**的通報義務，以及 **2027 年 12 月**的完整技術合規。

註記

歐盟執委會指引現況： 歐盟執委會於 2026 年 3 月 3 日發布 CRA 指引草案。意見徵詢已於 2026 年 4 月 13 日結束。這不是最終指引，但對市場投放、自由與開源軟體、支援期間、實質修改、產品分類、元件盡職調查、遠端資料處理、漏洞處理，以及與其他 EU 法規重疊時的規劃，仍是有用的參考資料。AI Act 與 DORA 的邊界問題可能仍需要後續指引。

2024 年 12 月 10 日

生效

過渡期開始

2026 年 6 月 11 日

公告機構

第 IV 章開始適用

2026 年 9 月 11 日

通報

第 14 條通報開始

2027 年 12 月 11 日

完整適用

技術要求、CE 標章、文件與符合性評鑑

先做這件事

先從通報準備開始。第 14 條期限早於完整技術合規，而且適用於已在 EU 市場上的適用範圍產品。

由於通報自 **2026 年 9 月 11 日**開始，通報準備應是第一個執行工作流：**偵測、分級、使用者通知與主管機關通報**必須在完整技術合規期限前可以運作。

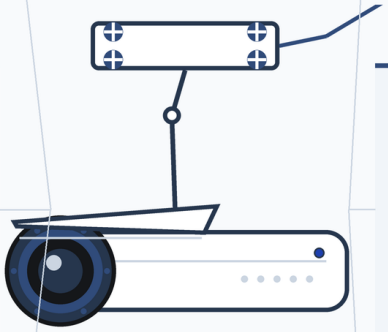
2027 年 12 月 11 日前已上市的數位元素產品，只有在該日後發生**實質修改**時，才適用 CRA 技術要求。通報義務不同。第 14 條適用於**所有適用範圍產品**，包括已在 EU 市場上的產品。

CRA 貫穿產品生命週期

步驟 01
界定產品範圍
適用範圍、分類、支援期間與風險評估

步驟 02
安全開發
安全預設、程式碼分析、SBOM 與相依性控管

步驟 03
驗證並文件化
安全測試、弱點分流、技術文件與使用者說明



步驟 04
投放市場
EU 符合性聲明、CE 標誌與發布決策

步驟 05
監控並更新
CVE、公告、利用活動、安全更新與揭露

步驟 06
支援並合作
第14條通報、使用者通知、主管機關要求與支援終止

連網 IP 攝影機，從產品規劃到 CRA 下的上市後支援

適用範圍內的產品

適用範圍與排除

CRA 適用於硬體與軟體產品，只要其預期用途或可合理預見用途包含與裝置或網路的直接或間接資料連線。範圍涵蓋電腦、智慧型手機、網路設備、IoT 裝置、工業控制系統與資料處理應用程式。

以下類別明確排除：

- 受 EU 規則 2017/745 與 2017/746 規範的醫療器材與體外診斷醫療器材
- 受 EU 規則 2019/2144 規範的汽車系統
- 受 EU 規則 2018/1139 規範的航空設備
- 受指令 2014/90/EU 規範的船舶設備
- 僅為國家安全或國防目的開發的產品
- 沒有數位元素或網路連線的純機械產品

除非有明確排除事由，連網產品應先按適用範圍產品處理。

註記

客製化產品：狹義的例外規定。 如果產品是依書面合約，針對某一特定企業使用者量身打造，可以在兩項要求上採取不同作法：預設安全組態（仍須提供回到原始安全狀態的途徑），以及免費安全更新（合約可另行約定商業條件）。其餘要求全部仍適用：漏洞處理、其他產品安全要求、第 14 條通報、技術文件、CE 標章、符合性評鑑與支援期間。這不是一般的 B2B 例外規定，也不涵蓋銷售給企業的現成產品。

經濟營運者責任

製造商	設計安全產品、評估風險、準備技術文件、執行符合性評鑑、處理漏洞，並通報第 14 條事件。
進口商	檢查製造商合規狀態、驗證 CE 標章與文件、確保聲明可供查閱，並處理已知漏洞。
經銷商	供應前檢查注意義務項目、驗證必要資訊與說明，避免供應不合規產品。

產品分類決定評鑑路徑

產品類別決定如何證明符合性。

類別	範例	符合性評鑑
預設「未分類」	不屬於重要或關鍵類別的一般軟體與連網消費性產品	模組 A：自我評鑑
重要「Class I」	身分管理、瀏覽器、密碼管理工具、防毒、VPN、網路管理、路由器、智慧門鎖、安全攝影機等類似產品	只有在依要求適用相關調和標準、共同規格或認證方案時，才可採模組 A；否則採模組 B+C 或模組 H
重要「Class II」	Hypervisor、容器執行環境、防火牆、IDS/IPS，以及防竄改微處理器	模組 B+C、模組 H，或保證等級至少為「substantial」的適用歐洲資安認證方案
關鍵產品	安全元件、智慧卡、智慧電表閘道器、硬體安全盒	在要求且可取得時採歐洲資安認證；否則採 Class II 路徑

四大產品類別

上方表格為範例。下方則為完整參考清單，請對照產品核心功能進行判斷。

預設產品

多數產品落於此類別。任何數位元素產品，其核心功能不符合下方重要或關鍵清單條目者，視為預設產品。符合性路徑為模組 A 自我評鑑。

常見範例：

- 智慧電視與串流裝置。
- 網路印表機與多功能辦公室設備。
- 藍牙喇叭與消費性音訊產品。
- 媒體播放器軟體應用程式。
- 遊戲主機、電子書閱讀器與類似消費性電子產品。
- 不含資安功能的智慧型廚房家電，例如烤箱、冰箱與洗碗機。
- 不含資安功能的智慧型燈泡與連網照明。
- 不具健康監測用途的健身追蹤器。
- 不屬於瀏覽器、密碼管理工具或 VPN 應用程式的一般用途行動應用程式。
- 文書處理與試算表等辦公室生產力軟體。

上方清單僅供參考說明。下方重要與關鍵清單則為完整列舉。

重要產品（Class I）

強制第三方評鑑，除非依要求適用相關調和標準、共同規格或認證方案。

1. 身分管理與特權存取管理軟硬體，包括驗證與存取控制讀取器（含生物辨識讀取器）。
2. 獨立式與內嵌式瀏覽器。
3. 密碼管理工具。
4. 搜尋、移除或隔離惡意軟體的軟體。
5. VPN 產品。
6. 網路管理系統。
7. 資安事件管理（SIEM）系統。
8. 開機管理程式。
9. 公開金鑰基礎建設與數位憑證發行軟體。
10. 實體與虛擬網路介面。
11. 作業系統。
12. 用於連接網際網路的路由器、數據機，以及交換器。
13. 具資安相關功能的微處理器。
14. 具資安相關功能的微控制器。
15. 具資安相關功能的 ASIC 與 FPGA。
16. 智慧家庭一般用途虛擬助理。

17. 具資安功能的智慧家庭產品（智慧門鎖、安全攝影機、嬰兒監視系統、警報系統）。
18. 具互動功能（語音、攝影、定位追蹤）的網路連線玩具。
19. 具健康監測用途的個人穿戴裝置（在 EU 規則 2017/745 或 2017/746 不適用時），或預期供兒童使用的穿戴裝置。

重要產品（Class II）

強制第三方評鑑，較嚴格路徑。即使有調和標準也不得採自我評鑑。

1. 支援作業系統與類似環境虛擬化執行的 Hypervisor 與容器執行環境系統。
2. 防火牆、入侵偵測與防禦系統。
3. 防竄改微處理器。
4. 防竄改微控制器。

關鍵產品

在認證方案可取得時，要求歐洲資安認證。否則採 Class II 路徑。

1. 含安全盒的硬體裝置。
2. 指令 (EU) 2019/944 第 2 條第 23 點所定義之智慧計量系統內的智慧電表閘道器，以及用於進階資安目的（包括安全密碼處理）的其他裝置。
3. 智慧卡與類似裝置，包括安全元件。

如果產品的核心功能符合重要或關鍵清單中的條目，產品就屬於該類別。如果產品將清單中的條目整合為元件，但自身核心功能屬於其他類別，則整合不會改變產品類別。

如何分類：以核心功能而非整合元件為依據

上方清單告訴你類別有哪些。但沒有告訴你如何套用到自己的產品。CRA 的答案是一個關鍵詞：**核心功能**。

產品的類別由其核心功能決定，而不是由整合了哪些元件決定。將核心功能對照重要清單，產品就是重要產品（Class I 或 Class II）。對照關鍵清單，產品就是關鍵產品。兩者皆不符合，產品就是預設產品。這就是整個測試。

實務上的保險條款落在第 7 條第 1 項的第二句。整合重要元件並不會讓整合產品本身被歸入重要類別。在智慧家庭中樞嵌入防火牆程式庫，不會讓中樞變成防火牆。前言第 45 點以直白方式說明：防火牆與入侵偵測系統屬於重要 Class II，但碰巧整合它們的其他產品則不屬於此類。

請使用以下順序進行自我分類。

1. **用一句話描述產品的核心功能。** 如果做不到，後續分析就無法成立。重點放在產品缺了什麼就無法運作。
2. **對照上方重要清單。** 命中 Class I 或 II 表示產品屬於重要類別。
3. **對照上方關鍵清單。** 命中表示產品屬於關鍵類別。在認證方案可取得時採歐洲資安認證路徑；否則採 Class II 路徑。
4. **兩份清單都不符合。** 產品屬於預設類別。符合性路徑為模組 A 自我評鑑。
5. **記錄判斷理由。** 一頁備忘錄，包含核心功能描述、清單比對結果與所選路徑，應納入技術檔案。

兩個實作範例。

內嵌密碼管理元件的智慧家庭中樞。 核心功能：協調家中消費性 IoT 裝置的自動化情境。密碼管理元件由其供應商獨立銷售，本身屬於重要 Class I 產品。中樞的核心功能是居家自動化，不是憑證管理。中樞仍屬於預設類別。

以功能集判斷的作業系統。 某產品以智慧家庭家電的形式行銷，但主要功能為硬體與週邊初始化、程序排程、記憶體管理與系統呼叫介面。這就是作業系統的核心功能。作業系統屬於重要 Class I 產品。不論行銷方式為何，該產品就是重要 Class I。

如果分類結果讓團隊其他成員感到意外，核心功能描述需要在出貨前再檢視一次。

雲端服務何時納入產品範圍

多數數位元素產品都會依賴裝置以外的服務：雲端後端、行動隨身應用程式、空中更新伺服器、驗證入口、裝置管理系統。CRA 不會把這些都視為產品的一部分。只有同時滿足下列兩項條件時，這些服務才會被視為產品的一部分：

- 該軟體是**由你的團隊設計與開發，或在你的責任下進行**。
- 沒有該服務，**產品就無法執行其中一項功能**。

如果其中一項條件不符合，遠端服務就落在 CRA 產品邊界之外。你不擁有但產品會連線的第三方 SaaS，不屬於你的產品。宣傳產品但不支援其功能的網站，也不屬於你的產品。

當遠端元件納入範圍時，是**作為產品的一部分**納入。技術檔案、符合性評鑑、符合性聲明、漏洞處理與第 14 條通報時程，都同時涵蓋雲端元件與裝置。

請使用以下對照表快速判斷。

元件	是否屬於產品範圍？
與裝置配對的行動隨身應用程式	**是。** 由你設計，且裝置缺了它就無法設定或使用。
儲存與處理裝置資料的雲端後端	**是。** 由你設計，且儀表板或主要功能缺了它就無法運作。
空中更新伺服器	**是。** 由你設計，且裝置缺了它就無法接收安全更新。
控制裝置存取的驗證入口	**是。** 由你設計，且使用者缺了它就無法登入。
產品的行銷網站	**否。** 並未支援產品功能。
產品整合的第三方 SaaS（非你所擁有）	**否。** 不是你設計的。第三方服務提供者依 NIS 2 承擔其自身義務。
你的服務運作所在的一般雲端基礎設施（IaaS 或 PaaS）	**否。** 不是你設計的。基礎設施提供者落於 NIS 2 範疇。

常見案例：智慧家庭裝置配合行動應用程式、更新伺服器與雲端後端。三者皆由製造商設計，且裝置缺了任何一者就無法執行其宣稱功能。三者都屬於產品範圍。CRA 義務適用於整個組合。如果雲端後端再與第三方分析 SaaS 連線，該 SaaS 不屬於產品。第三方服務提供者依 NIS 2 承擔其自身義務。

CRA 並未要求對製造商的網路與資訊系統整體採取資安措施。它要求的是屬於產品一部分的遠端服務的安全。界線是產品邊界，不是公司邊界。

你的供應鏈：CRA 下的角色分工

CRA 將主要義務放在製造商身上，但進口商與經銷商也承擔影響產品上市方式的義務。對你而言，有三件事需要知道。

角色	供應前驗證項目	發現漏洞時的作法	何時承擔你的義務
進口商	CE 標章、EU 符合性聲明、正確語言的使用者說明、產品上或隨附的你方聯絡資訊	不延遲地告知你；若產品有重大資安風險，則直接通報市場監督機關	以自身名稱或商標投放你的產品，或對產品進行實質修改時
經銷商	CE 標章、確認你與進口商已盡其義務、產品隨附必要文件	不延遲地告知你；若產品有重大資安風險，則直接通報市場監督機關；可停止供應產品	與進口商相同的觸發條件

對製造商而言，這意味三件實務工作：

- 你的 CE 標章、EU 符合性聲明與使用者說明，在經銷商檢查的當下，必須正確且以正確語言提供。通路夥伴有驗證義務，缺漏或錯誤時可以拒絕供應產品。
- 你需要清晰、低門檻的聯絡途徑，讓進口商與經銷商可以將漏洞通報納入你的漏洞處理流程。他們會主動使用。
- 任何將你的產品改貼自有品牌、以自身名稱或商標投放，或進行實質修改的合作夥伴，就會變成該版本的製造商。完整的技術檔案、符合性評鑑、通報與支援期間義務，將轉移到他們身上。詳見下節《當其他人成為製造商》中的實質修改規則。

實質修改：何時需要重新進行符合性程序

產品上市後，CRA 將後續變更分為兩類。多數變更屬於例行性，不需要額外作業。部分變更屬於實質修改。實質修改在 CRA 下視為新產品上市。也就是說，需要重新進行符合性評鑑、更新技術檔案、簽署新的符合性聲明，並在新版本上加貼 CE 標章。

判斷標準很簡短，落在實質修改的定義中。若下列任一條件成立，即屬實質修改：

- 變更**影響符合性**，無法繼續符合基本資安要求。
- 變更**修改了預期目的**，與原評鑑時不同。

兩者皆不符合時，變更不屬於實質修改。仍應記錄判斷理由並存檔。分析本身就是證據鏈的一部分。

不屬於實質修改的情況

兩種例外規定處理多數實務情況。

降低資安風險、且不改變預期目的的安全更新與錯誤修正，不屬於實質修改。修補已知漏洞、調整輸入驗證以解決缺陷，或為了處理 CVE 而重建元件，都屬於這一類。

翻新、維護與維修也不自動構成實質修改。只有在改變預期目的，或影響基本資安要求符合性時，才會構成實質修改。

小幅使用者介面工作也是安全的一邊。新增語言、替換圖示集，或調整畫面排版，本身不屬於實質修改。新增需要適當輸入驗證的輸入元素，則可能構成實質修改。

備品

CRA 以狹義且具體的方式排除備品。**相同備品**，即依與所取代元件相同規格製造者，完全落於規則範圍之外。功能性替代品則不在此列。

請使用以下對照表快速判斷。

替代品	主機在 2027 年 12 月 11 日前上市	主機在 2027 年 12 月 11 日或之後上市
與原元件**相同**、規格一致	備品落於 CRA 範圍外。更換不觸發任何義務。	備品落於 CRA 範圍外。更換不觸發任何義務。
功能等同，但設計或規格不同	替代品本身為 CRA 產品。主機因早於適用日期而無 CRA 義務。	替代品為 CRA 產品。需依上方兩段測試評估更換到主機是否構成主機的實質修改。

兩項實務影響。第一，排除規定取決於規格相同。即使客戶無法察覺差異，採用不同晶片組重建的無線模組仍不算相同備品。第二，供應功能性替代品的製造商，無論主機由誰製造，都承擔該零件的 CRA 義務。

軟體更新與功能開關

軟體發布是實質修改問題最常見的來源。仍以兩段測試處理。

修補漏洞的修補程式不屬於實質修改。啟用產品從未被評鑑過的能力的功能開關，則屬於實質修改。讓產品可依據新類別輸入做決策的模型升級也是。如果某次發布同時包含修補與新功能，請針對新功能進行評估。

是否捆綁不是關鍵。功能更新與安全修補一同發布或分開發布，與評估結果無關。

如果你採用功能開關或分階段推送，計算時點是在正式環境中對最終使用者啟用的時刻，而不是包含開關的二進位檔出貨時刻。

實務判斷流程

每次變更上線前，請依下列順序判斷。

1. **變更是否修改了產品的預期目的？** 若是：屬於實質修改。對新版本重新進行符合性評鑑。
2. **變更是否影響基本資安要求的符合性？** 若是：屬於實質修改。對新版本重新進行符合性評鑑。
3. **其他情況：** 不屬於實質修改。記錄分析後，繼續沿用現有技術檔案。

如果產品屬於重要或關鍵類別，且原本就採第三方評鑑路徑，實質修改會讓你回到相同路徑。對於可能屬於實質修改的變更，請提前通知第三方。自我評鑑不是事後為重要產品重新分類的後門。

構成實質修改後的後果

實質修改視為新產品上市。對製造商而言：

- 更新已變更版本的技術文件。
- 依產品類別所要求的路徑，重新進行符合性評鑑。
- 為已修改版本核發新的 EU 符合性聲明。
- 重新加貼 CE 標章，並存檔新的聲明。
- 在完整保存期間內，保留先前版本的文件。新版本不會抹去舊版本。

對軟體產品而言，可在支援期間內將安全更新範圍限定為已上市的最新版本，前提是舊版本使用者可以免費、且無需新硬體就能升級到最新版本。

依先前符合性程序售出的現場單位不受影響。義務適用於被供應的已修改版本，而非早於此之前的相同單位。

當其他人成為製造商

如果你並非原始製造商而執行實質修改，CRA 將你視為該版本的製造商。第 13 條與第 14 條的完整義務轉移至你。同樣規則適用於以自身名稱或商標投放產品的情況。

這捕捉到的情境比團隊預期的更多：

- 系統整合商出貨包含新功能的客製化韌體建置。
- 經銷商以自有品牌貼標產品，並改變所宣傳的預期目的。
- 服務提供者將第三方裝置與自家韌體捆綁銷售。

在這些情境中，執行變更者就繼承該版本的製造商義務：技術檔案、符合性評鑑、通報、漏洞處理等。一旦跨越任一條線，「進口商」或「經銷商」的角色標籤就不再具保護作用。

需要準備的項目

本節可作為工作檢查表。後續章節會逐項說明各項要求的細節。

資安風險評估

產品上市前，需要在檔案中保存一份資安風險評估。這是用你自己的話，解釋為何產品可以安全出貨並維持在市場上的文件。

評估應涵蓋：

- 產品的預期目的，以及可合理預見的使用情境
- 產品將運作的條件與環境
- 需要保護的資料與功能
- 適用的威脅，以及用來管理威脅的控制措施
- 產品預期使用時間

多數團隊的結構作法。 可信賴的方法論方向一致：識別資產（產品處理的資料、金鑰與憑證等資安材料、損失將傷害使用者的功能），對應各資產的存放或流動位置，依資產與環境建立威脅模型，並以機密性、完整性、可用性作為維度，評分衝擊與可能性，決定哪些剩餘風險可接受、哪些須緩解，並於每輪控制後重新評估（每個新增的金鑰、憑證或驗證功能本身就是一項待分析的新資產）。

威脅建模。 上述第三步是最技術性的工作，自有成熟技術。STRIDE 將威脅分類為 spoofing、tampering、repudiation、information disclosure、denial of service 與 elevation of privilege；使用廣泛，適用多數連網產品。LINDDUN 為處理個人資料的產品擴展視角，增加 linkability、identifiability、non-repudiation、detectability、disclosure of information、unawareness 與 non-compliance；在資料保護與 CRA 義務交疊處有用。PASTA 採七階段流程，從業務目標走到剩餘風險接受；對於攻擊圖像驅動設計的複雜系統有用。這些方法都不是 CRA 特有的，CRA 也不要求採用任何特定一種。請依產品暴露面選擇合適者。

完整方法論可參考的來源。 CRA 並未規定方法。德國聯邦資訊安全局（BSI）發布 技術指引 TR-03183，是目前公開流通中最詳細、與 CRA 對齊的風險評估方法論。ENISA 則發布更廣泛的 CRA 實作指引。

支援期間內請持續更新評估。威脅圖像、元件或使用情境改變時，評估也應隨之更新。

支援期間決定

每項產品都需要設定支援期間，並在購買時公布結束日。支援期間是你處理漏洞、出貨安全更新，並維持技術文件最新的時間窗。

期間長度

至少 5 年。如果產品預期使用時間不足 5 年，支援期間應與預期使用時間一致。若預期使用時間更長，支援期間就應反映該較長使用時間；路由器、作業系統與工業控制器這類產品，通常需要超過 5 年。

衡量因素

設定期間時，需以合比例方式納入：

- 使用者對產品的合理期待

- 產品性質，包括預期目的
- 已為該類產品設定產品壽命的 EU 法規
- 市場上可比較產品的支援期間
- 產品依賴的運作環境的可取得性
- 提供核心功能的整合元件的支援期間
- 該產品類別的 ADCO 或執委會指引

所選期間的判斷理由必須納入技術檔案。市場監督機關可要求查閱。

必須公布的事項

在購買時，以易於存取的方式載明支援期間結束日，至少精確到月份與年份。若產品具有使用者介面，請在支援期間屆滿時顯示通知。

更新保留

支援期間內提供給使用者的每項安全更新，必須在發布後至少 10 年，或在支援期間剩餘期間內維持可用，兩者取較長者。

元件盡職調查

產品由元件組成。有些是自行撰寫的，有些是採購而來，有些則來自開源儲存庫。CRA 將產品視為整體進行合規評估，所以元件也算在內。如果某元件存在漏洞，你的產品就存在漏洞。如果某元件沒有安全更新，你的產品也就沒有。

製造商必須對第三方元件，包括自由與開源元件，執行盡職調查。元件不得危害產品的資安。

盡職調查的程度應依元件所帶風險的合比例方式進行。處理驗證的程式庫，與字型渲染程式庫不能等同對待。請依風險合比例採用下列一項或多項檢查：

1. **檢查元件的 CE 標章。** 若元件本身為 CRA 產品，且供應商已證明符合性，元件上會有 CE 標章。這表示供應商已完成自身的 CRA 工作。
2. **檢查安全更新歷史。** 持續推出安全更新的元件，比沉寂多年的元件風險更低。請關注發布節奏與近期資安公告紀錄。
3. **對照漏洞資料庫檢查元件。** 歐洲漏洞資料庫與公開 CVE 資料庫，可以告訴你元件的已知狀況。已知 CVE 而無修補，是明顯的警訊。
4. **執行額外的資安測試。** 上述不足時，請在整合情境中測試元件：靜態分析、動態分析、模糊測試或聚焦的資安審查。

對於在供應商完全納入 CRA 前就已整合（因此尚未取得 CE 標章）的元件，請改用其他三項檢查。盡職調查義務不會因為供應鏈尚在追趕而暫停。

檔案需保存的證據

技術檔案需要證明盡職調查已執行，而非僅聲稱。請保存：

- 產品中第三方元件清單，可追溯至版本，包括開源元件。SBOM 是自然的存放位置。
- 你檢視過的供應商安全文件：資安政策、漏洞揭露計畫、支援期間承諾。
- 顯示元件在產品中安全運作的整合測試報告。
- 與商業供應商的合約或 SLA 中的資安條款：漏洞通知時程、支援期間承諾、升級規則。

- 元件盡職調查發現限制時，所新增的產品層級緩解措施紀錄：沙箱、限縮權限、輸入驗證、網路分段。

在元件中發現漏洞時

如果盡職調查或上市後監控發現元件中的漏洞，你必須做兩件事。第一，通知維護該元件的個人或單位。若元件為開源，則為上游專案。第二，在自家產品上以與處理任何其他漏洞相同的時程修補。如果你已開發出修補程式，請以機器可讀格式（如適用）與維護者分享程式碼或文件。

CRA 不允許你等待元件維護者行動後才保護自家使用者。產品的漏洞處理時程與上游獨立運作。

13 項產品安全要求

每項數位元素產品在上市時，以及在整個支援期間內，必須符合 13 項基本資安要求。它們是 CRA 下「資安」在產品層面的最低標準。

13 項要求為：

- 上市時沒有已知可利用漏洞
- 預設安全組態
- 安全更新，包括可選擇退出的自動更新
- 防止未授權存取
- 儲存、傳輸與處理資料的機密性
- 資料、韌體與組態的完整性
- 資料最小化
- 可用性與韌性，包括抵禦阻斷服務攻擊
- 不對其他連線裝置或網路造成負面影響
- 限縮攻擊面，包括外部介面
- 透過利用緩解機制降低事件影響
- 記錄資安相關活動，並提供使用者退出選項
- 安全且永久的資料刪除與可攜性

每項要求在本指南後續章節詳細展開，包括實務意義與應保存的證據。

8 項漏洞處理要求

製造商也需要在產品支援期間持續運作的漏洞處理流程：

1. 識別並記錄漏洞（包括軟體物料清單，SBOM）
2. 風險管理與及時安全更新
3. 定期安全測試
4. 安全更新與漏洞揭露通知
5. 協調式漏洞揭露（CVD）政策
6. 漏洞分享與通報聯絡窗口
7. 安全更新散布機制
8. 附帶建議訊息的免費安全更新

第 14 條通報時程

這些義務自 **2026 年 9 月 11 日**開始適用。它們適用於適用範圍內數位元素產品的製造商，也包括 **2027 年 12 月 11 日**前已上市的產品。微型與小型企業通常不會因此免除通報義務。小型企業的罰鍰減免範圍很窄，只涉及第一個 **24 小時早期警示期限**。

CRA 將漏洞狀態分為三層：

- **漏洞：** 可能被利用的弱點
- **可利用漏洞：** 在真實環境下可被利用的弱點
- **遭主動利用的漏洞：** 已確認被用於攻擊的弱點

何時開始計時

訊號出現的當下，計時尚未開始。在你完成初步評估、且對產品中存在遭主動利用的漏洞，或產品安全已遭嚴重事件危害有合理程度的確信後，才開始計時。重點在於迅速完成初步評估，而不是等待完整調查結束。如果客戶、研究人員、主管機關或其他第三方告知你潛在問題，請毫不延遲地評估，並在該評估提供合理確信時開始計時。

偵測到**遭主動利用的漏洞**時，適用下列通報時程：

時程	必要事項	通報位置
24 小時內	主動利用的早期警示通知	透過各國 CSIRT 向 ENISA 通報
72 小時內	漏洞通知：受影響產品、利用與漏洞的一般性質、緩解措施、使用者可採取的矯正措施，以及必要時的敏感性標示	透過各國 CSIRT 向 ENISA 通報
矯正或緩解措施可用後不晚於 14 天	最終報告：漏洞說明、嚴重程度、影響、惡意行為者的可用資訊，以及安全更新或其他矯正措施細節	透過各國 CSIRT 向 ENISA 通報

偵測到對產品安全有影響的**嚴重事件**時，適用下列通報時程：

時程	必要事項	通報位置
24 小時內	早期警示通知，包括該事件是否疑似由非法或惡意行為造成	透過各國 CSIRT 向 ENISA 通報
72 小時內	事件通知：事件性質、初步評估、緩解措施、使用者可採取的矯正措施，以及必要時的敏感性標示	透過各國 CSIRT 向 ENISA 通報
72 小時事件通知後 1 個月內	最終報告：詳細事件說明、嚴重程度、影響、可能威脅或根本原因，以及已採取或進行中的緩解措施	透過各國 CSIRT 向 ENISA 通報

通知會隨後續了解持續更新

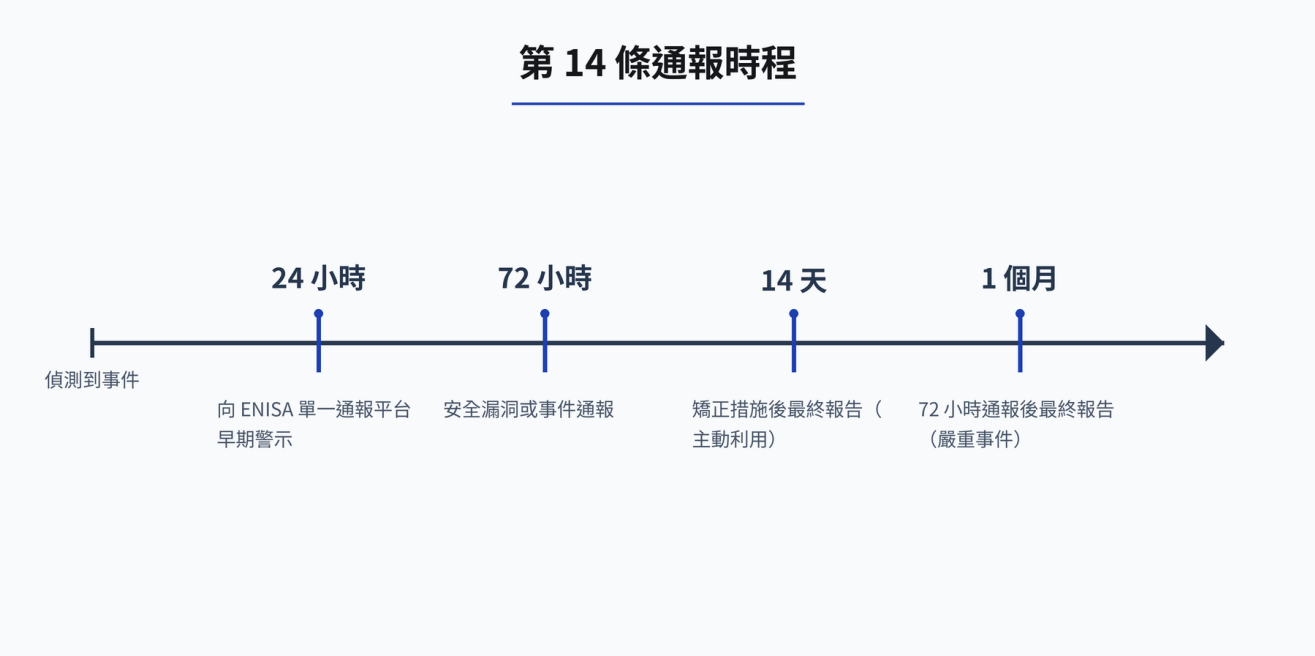
24 小時、72 小時與 14 天（或 1 個月）的提交，是同一通知的不同階段，而不是各自獨立的申報。每個階段補充前一階段尚未取得的資訊。被指定為協調者的 CSIRT 也可以隨時要求中間更新。你不需要重複已提供的資訊。

通報透過 **CRA 單一通報平台**提交，經由製造商主要成員國的國家電腦資安事件應變團隊（CSIRT）路由，ENISA 同時取得存取權。

告知使用者

知悉後，你必須告知受影響使用者，並於適當時告知所有使用者，說明漏洞或事件，以及可部署的風險緩解與矯正措施。這與公開揭露不同。義務是把資訊送到需要保護自身的使用者手上，並依風險合比例執行。對於用於敏感或關鍵環境的產品，在漏洞尚未緩解前，請將詳細技術資訊限於相關客戶；過早公開細節可能讓利用更容易。

漏洞修補或緩解完成後，較廣泛的揭露可能成為適當作法，幫助使用者驗證產品已不受影響，並提升整體警覺。請依剩餘風險合比例調整細節程度與時點。如果你沒有及時告知使用者，且 CSIRT 判斷此為合比例且必要時，CSIRT 可代為提供資訊。



遭主動利用的漏洞

24 小時	早期警示通知
72 小時	漏洞通知
矯正措施後 14 天	最終報告

嚴重事件

24 小時	早期警示通知
72 小時	事件通知
72 小時通知後 1 個月	最終報告

產品不符合性時的矯正行動

如果你知道或有理由相信你已上市的產品，或你的某項流程，與 CRA 基本資安要求不符，你必須立即採取行動。義務自上市起算，並持續整個支援期間。

三項選擇

1. **回復符合性。** 修補產品或流程。對軟體產品而言，通常是安全更新或流程變更。將修補套用到所有支援版本。
2. **撤回。** 停止在市場上供應產品。將其從供應鏈，以及任何持有庫存的零售商、整合商與經銷商處撤下。
3. **召回。** 從已持有的使用者手上取回產品。在使用者面臨的資安風險顯著、且僅憑修補或撤回不足時使用。

選擇應依風險合比例，而非固定順序。可修補且已有修補程式的漏洞通常代表「回復符合性」。無法在現場安全修補的產品通常代表「撤回」，而在風險顯著的使用中情境下則代表「召回」。

還必須執行的事項

- 當不符合性為遭主動利用的漏洞或嚴重事件時，**依第 14 條鏈通報**。通報時程如前文所述。
- **告知使用者**不符合性與可自行採取的矯正措施。合比例規則請參見前文《告知使用者》一節。
- **配合**市場監督機關所提的合理請求，包括以其可理解的語言提供技術文件。
- **保存證據。** 保留紀錄，呈現你發現的內容、何時發現、採取的處理，以及與使用者及主管機關的溝通。技術文件與 EU 符合性聲明必須在上市後至少 10 年，或在完整支援期間內維持可取得，兩者取較長者。

產品文件要求

文件必須在數位元素產品上市後至少保存 **10 年**，或在**完整支援期間**內保存，兩者取較長者。摘要層面上，技術文件需要 8 個證據家族：

1. 一般產品說明
2. 設計、開發與生產細節（包括 SBOM）
3. 資安風險評估
4. 支援期間決定
5. 已適用的調和標準與規格
6. 測試報告
7. EU 符合性聲明
8. 完整 SBOM（依市場監督機關要求提供）

符合性評鑑路徑檢查表

使用上方分類表識別路徑。接著將路徑決策與用來佐證的標準、規格、認證方案或公告機構證據，一併保存在技術檔案中。

實作範例。相同的分層結構適用於每項數位元素產品，不僅限於安全攝影機。

產品安全要求

a. 上市時沒有已知可利用漏洞

不要在公眾已知且可被利用的漏洞仍未處理時出貨。已知漏洞可能來自公開資料庫、供應商通知、客戶回報，或內部追蹤系統。

符合此要求的作法：

- 每次發布前檢查漏洞資料庫，包括 Common Vulnerabilities and Exposures（CVE）
- 在建置流程中使用靜態與動態應用程式安全測試（SAST/DAST）
- 對所有第三方與開放原始碼元件執行相依性掃描
- 針對每項已識別問題，記錄風險接受或緩解決策

b. 預設安全組態

產品在預設狀態下應可安全使用。關閉不必要服務，避免弱預設憑證，並讓任何不安全的啟用模式維持短暫且受控。預設組態義務在以書面合約供應給企業使用者的客製化產品上可另行約定，但回到原始安全狀態的途徑必須始終保留。

符合此要求的作法：

- 在預設建置中停用遠端存取連接埠與除錯介面
- 強制採用強固的預設驗證機制
- 將管理功能限制於已授權使用者
- 實作安全的出廠重設，將所有設定與韌體回復到已知安全狀態，同時移除使用者資料

c. 安全更新，包括可選擇退出的自動更新

產品需要可在部署後處理安全問題的修補機制。自動更新適用時，應預設啟用，並提供使用者清楚的延後或退出方式。

符合此要求的作法：

- 對更新套件實作密碼學簽章與完整性驗證
- 提供防回復機制與更新事件記錄
- 建立可通知使用者待安裝更新的系統
- 透過清楚的設定介面，讓使用者延後或停用自動更新

d. 防止未授權存取

存取控制需要保護本機與遠端介面。目標是阻止未授權使用者接觸功能、資料、組態或管理介面。

符合此要求的作法：

- 強制密碼複雜度政策與強固預設憑證
- 在適當情況下實作多因素驗證（MFA）
- 套用角色型存取控制（RBAC）與工作階段逾時處理
- 記錄失敗存取嘗試，以異常偵測標示未授權活動，並將這些事件提供給後續審視與通報

e. 儲存、傳輸與處理資料的機密性

敏感資料在靜態、傳輸與處理期間都需要保護。

符合此要求的作法：

- 使用標準化加密演算法，例如靜態資料採 AES-256，傳輸資料採 TLS
- 套用安全金鑰管理實務
- 將機密資料與非關鍵系統元件分離
- 保留所有資料存取事件的稽核日誌

f. 資料、韌體與組態的完整性

此要求涵蓋系統本身，例如韌體、軟體與組態檔案，也涵蓋系統處理的資料，例如量測值、控制命令與使用者輸入。

符合此要求的作法：

- 實作安全開機與簽章韌體，確保只執行受信任程式碼
- 使用執行階段驗證，偵測並回報竄改嘗試
- 套用密碼學雜湊與數位簽章，保護資料完整性
- 建立可跨系統或組織邊界產生、散布與驗證密碼金鑰的基礎設施

g. 資料最小化

只蒐集與處理產品預期目的所需的資料。這適用於個人資料與技術資料。

符合此要求的作法：

- 執行隱私衝擊評估，或設計階段資料保護檢查，以識別不必要的資料流
- 移除未使用的遙測、診斷或背景資料蒐集，或將其設為選用
- 實作可設定的資料蒐集選項，讓延伸蒐集可依情境開啟或關閉

h. 可用性與韌性，包括抵禦阻斷服務攻擊

在事件或攻擊期間，關鍵產品功能應維持可用，或以受控方式失效。

符合此要求的作法：

- 實作斷路器、重試邏輯、備援機制與 watchdog timer
- 套用資源限制，避免資源耗盡
- 使用速率限制與輸入驗證，防範阻斷服務情境
- 套用網路層過濾，封鎖過載嘗試

i. 不對其他連線裝置或網路造成負面影響

產品不應干擾同一環境中的其他系統。它應以可預測方式運作，並避免過度使用共享資源。

符合此要求的作法：

- 實作流量整形，並限制廣播或多播使用
- 確保符合通訊協定規格
- 使用自我監控，偵測並防止網路泛洪或資源耗盡等干擾行為

j. 限縮攻擊面，包括外部介面

將進入點與暴露功能降至最低。這包括實體連接埠、無線介面、API、除錯服務與不必要軟體元件。

符合此要求的作法：

- 在正式建置中停用未使用的服務、連接埠與介面
- 強化系統預設值，並限制使用者權限
- 將軟體架構模組化，使元件彼此隔離
- 套用安全軟體設計原則，並透過威脅建模識別與移除不必要暴露

k. 透過利用緩解機制降低事件影響

設計時應假設部分攻擊會成功。產品設計要限制損害擴散範圍。

符合此要求的作法：

- 分離系統元件，並使用沙箱或容器化讓元件在隔離環境中執行
- 強制權限分離，使關鍵功能以所需最低權限執行
- 設計時確保單一元件遭入侵，不會讓攻擊者控制整個系統

l. 記錄資安相關活動，並提供使用者退出選項

記錄存取嘗試與資料修改等資安相關活動，使其可供監控與稽核。CRA 要求時，需要提供使用者退出機制。

符合此要求的作法：

- 實作結構化日誌，例如含時間戳記的 JSON 日誌
- 提供具日誌輪替的本機日誌儲存，以及遠端日誌串流選項
- 監控登入嘗試、組態變更與軟體更新等事件中的異常
- 在允許情況下，提供清楚的使用者介面停用日誌記錄

m. 安全且永久的資料刪除與可攜性

使用者需要實用方法永久移除資料與設定。資料可移轉至另一項產品或系統時，移轉也必須安全。

符合此要求的作法：

- 實作安全抹除功能，覆寫儲存區域或以密碼學方式刪除金鑰
- 使用已驗證且加密的通道進行資料可攜性移轉，避免移轉期間暴露

漏洞處理要求

1. 識別並記錄漏洞

你需要知道產品包含哪些軟體元件，以及哪些已知漏洞會影響它們。軟體物料清單（SBOM）提供機器可讀的元件盤點。

符合此要求的作法：

- 將 SBOM 產生直接整合到 CI/CD 流程，使每次建置都產出最新元件清單
- 使用 CycloneDX、SPDX 或 SWID 等既有格式，確保互通性
- 對 CVE 清單，以及 CISA KEV、ENISA EUVD 等資料庫執行自動漏洞掃描
- 在整個支援期間將 SBOM 作為技術文件的一部分維護，並依市場監督機關要求提供

2. 風險管理與及時安全更新

發現漏洞時，要快速修補並交付安全更新。可行時，將安全修補與功能更新分開，使關鍵修補可迅速安裝。

符合此要求的作法：

- 設計更新機制，使安全修補不需完整系統更新即可推出
- 調整軟體與韌體結構，使關鍵元件可獨立修補
- 透過具完整性檢查的安全通道交付更新
- 保留更新活動記錄，以支援可追溯性並證明合規

3. 定期安全測試

安全測試不是一次性工作。威脅、相依項目與產品行為會變化，因此要在生命週期中持續測試。測試類型與頻率應由風險評估決定。

符合此要求的作法：

- 執行滲透測試，模擬真實攻擊
- 套用靜態與動態程式碼分析，識別安全弱點
- 使用 fuzz testing 找出輸入處理缺陷
- 正式排程並記錄安全程式碼審查與架構審查，尤其是在重大設計或功能變更後

4. 漏洞接收、CVD 政策與資安公告

涵蓋接收、協調式揭露與資安公告的義務（即前述摘要的第 4、5、6 項），實務上這些屬於同一個工作流程。

CRA 對於漏洞相關溝通設有三項各自獨立的要求：讓他人通報問題的途徑、協調式揭露政策，以及在出貨修補時發布資安公告。以下說明各項義務的內容。

接收

提供通報者清楚、低門檻的途徑。公開可見的漏洞通報聯絡方式（專用電子郵件或網頁表單）。支援安全通訊，例如公開 PGP 金鑰。此義務涵蓋對自家產品與其所含第三方元件的通報。

分級

對每件通報致謝，於追蹤系統中登錄、指派審查，並在定義期限內解決。將確認與狀態更新回覆給通報者。問題位於第三方元件時，請與上游維護者並行處理，與自家修補同步進行。

協調式漏洞揭露政策

公開 CVD 政策，為通報者與合作夥伴設定預期：聯絡方式、預期回應時間、你的承諾，以及對對方的期望。在保護使用者的同時，協調揭露並承認通報者貢獻。

修補後的資安公告

修補可用後，請對已解決問題發布資安公告。包含 CVE 識別碼、受影響產品版本、標準化嚴重程度（例如 CVSS），以及對使用者應採取行動的清楚、可取得資訊。以技術管理者與非技術使用者都能理解的語言撰寫。

延後公開揭露

只有在有正當理由認為立即揭露的資安風險超過利益，且僅延後至使用者有機會套用修補為止時，才得延後公開揭露。請記錄判斷理由。

5. 安全更新散布機制

更新機制需要可靠且能抵抗竄改。自動更新在技術上可行時，可縮短使用者暴露於風險中的時間。

符合此要求的作法：

- 透過安全通道傳送更新，並以數位簽章驗證
- 以可防止不完整或毀損安裝的方式套用更新
- 使用差異更新或模組化更新，降低中斷並更快交付修補
- 保留更新日誌，讓使用者或管理者可驗證更新狀態

6. 附帶建議訊息的免費安全更新

安全更新應迅速且不另收費交付，客製化企業產品另有協議者除外。每次更新都需要清楚的建議訊息，告知使用者變更內容與應採取行動。

符合此要求的作法：

- 維持可依產品情境直接通知使用者或自動套用更新的散布系統
- 以技術與非技術使用者都能理解的語言撰寫建議訊息
- 在相關時，於建議訊息中包含嚴重程度資訊
- 告知使用者應採取的行動，例如套用更新、變更組態或留意被入侵跡象
- 修補可用後不延遲地散布安全更新，避免使用者在修補已存在時仍處於暴露狀態
- 透過製造商所控管的通道發布資安公告，並從產品支援頁面連結至公告

免費與不延遲的義務於宣告的支援期間內持續適用。客製化產品的例外規定僅改變商業條件；資安公告義務仍適用。

技術檔案應包含的內容

技術文件

技術文件是 CRA 合規的核心證明。它需要涵蓋用來滿足基本資安要求的設計、技術與作業措施。技術文件必須在**上市前**存在，並在整個**支援期間**維持最新。

工程工作流中的技術檔案證據

步驟 1	**界定範圍與分類**	產品目的、預期用途、市場投放決策、產品分類、標準適用路徑。
步驟 2	**架構與風險**	架構、資料連線、使用條件、風險評估、緩解措施。
步驟 3	**元件與 SBOM**	機器可讀 SBOM、第三方元件、供應商輸入、漏洞追蹤。
步驟 4	**建置、測試、更新**	安全預設值、強化、測試報告、安全更新機制、建議訊息。
步驟 5	**發布與支援**	使用者說明、EU 符合性聲明、CE 證據、支援期間依據、更新記錄。

技術檔案有 8 項必要組成。它們共同說明**產品是什麼**、**如何建置與測試**、**考量了哪些風險**、**適用了哪些標準**，以及**上市後將如何支援**。你不需要照搬法律標題，但每項主題都必須涵蓋。

編號	組成項目	必須包含的內容
1	一般產品說明	預期目的與功能、相關軟體版本、照片或圖示（硬體適用）、使用者資訊與說明
2	設計、開發與生產細節	架構說明（元件與互動）、軟體物料清單（SBOM）、漏洞處理流程（CVD 政策、聯絡窗口、安全更新機制）、包含驗證的生產與監控流程
3	資安風險評估	已記錄的產品風險分析、各項基本資安要求如何適用於產品的說明、已識別風險的緩解
4	支援期間決定	記錄設定支援期間所用因素，例如使用者期待、可比較產品與法律指引
5	已適用的調和標準與規格	已適用調和標準、共同規格或 EU 認證方案清單；標示完整或部分適用；未適用標準時的替代解決方案
6	測試報告	產品與漏洞處理流程的符合性證據
7	EU 符合性聲明	將技術檔案連結至 CE 標章義務的聲明副本
8	完整 SBOM（依要求）	市場監督機關可要求完整 SBOM，以驗證合規

單一整合的技術檔案可以同時涵蓋 CRA 與其他適用 EU 法規（例如無線電設備指令或 ESPR），但前提是納入所有適用義務。

EU 符合性聲明

EU 符合性聲明是製造商正式聲明產品符合適用 CRA 資安要求的文件。每份聲明必須包含：

- 產品名稱、型式與唯一識別碼
- 製造商名稱與地址，或授權代表
- 由提供者承擔單獨責任的聲明
- 確保可追溯性的產品說明，可選擇包含圖片
- 明確聲明符合相關 EU 法規
- 所使用調和標準、規格或認證的參照
- 涉及的公告機構細節（名稱、編號、流程、證書編號）
- 簽署欄位：地點、日期、姓名、職務與簽名

簽署後，聲明具有法律拘束效果，並確認製造商對資安合規承擔完整責任。

包裝或手冊可使用簡化聲明，形式如下：「［製造商］特此聲明，產品［型式／名稱］符合 EU 規則 2024/2847。EU 符合性聲明全文可於以下網址取得：［網址］。」此簡化形式維持透明度，同時降低文件負擔，特別適合小型製造商或多產品組合。

使用者資訊與說明

使用者資訊與說明是合法上市的條件。製造商必須讓說明至少可取得 **10 年**，或在**完整支援期間**內可取得。進口商與經銷商在上市或供應產品前，需要確認說明存在、維持最新，且以正確 EU 語言提供。

使用者說明必須包含：

- 製造商身分與聯絡資訊
- 漏洞通報單一聯絡窗口
- 產品識別、預期目的與安全使用情境
- 已知或可預見的網路風險
- EU 符合性聲明連結
- 支援條件與明確支援結束日
- 設定、更新、安全使用、汰除，以及在適用時整合與 SBOM 存取的逐步安全說明

選擇正確的符合性評鑑路徑

模組 A：自我評鑑

模組 A（內部控制）允許製造商自行證明產品符合基本資安要求，並對設計與生產承擔完整責任。此路徑適用於預設（未分類）產品的製造商。重要 Class I 產品只有在相關調和標準、共同規格或歐洲資安認證方案可用，且依 CRA 路徑規則要求適用時，才可採用此路徑。

在模組 A 下，必須：

- 準備完整技術文件
- 詳述產品設計、生產流程、資安機制與漏洞處理流程
- 在產品生命週期中維持持續合規責任

- 在產品運作期間實作安全更新與漏洞管理計畫
- 保持記錄至少 10 年可供查閱

模組 B 與 C：以產品為中心的評鑑

模組 B 與 C 適用於需要針對特定產品型式進行第三方驗證的情況。它們適用於製造商未適用、僅部分適用，或無法適用相關調和標準、共同規格或認證方案的重要 Class I 產品。對重要 Class II 產品，製造商必須採用模組 B+C、模組 H，或保證等級至少為「substantial」的適用歐洲資安認證方案。

模組 B（EU 型式審查）： 公告機構審查代表性產品樣本與相關技術文件。它會驗證所有基本資安要求的符合性，並在產品設計符合 CRA 標準時，核發 EU 型式審查證書。

模組 C（型式符合，生產控制）： 製造商確保所有生產單位都符合模組 B 認證的核准型式。製造商加貼 CE 標章、發布 EU 符合性聲明，並保留記錄至少 10 年。模組 B 與 C 合併使用，可確認特定產品型號在技術上合規，且每一生產批次都維持與核准設計一致。

模組 H：以流程為中心的評鑑（完整品質保證）

模組 H（完整品質保證）聚焦於製造商整體內部品質系統，而非個別產品測試。它可用於重要 Class I 與 Class II 產品。關鍵產品在相關條件滿足時採認證路徑；條件未滿足時，採重要 Class II 產品可用的相同路徑。

在模組 H 下，必須：

- 建立並維持涵蓋整個產品類別的品質系統，包括設計、開發、生產、測試與漏洞處理
- 將品質系統提交公告機構評估與核准
- 接受公告機構的持續監督（稽核、檢查與流程審查），以驗證持續合規

核准後，製造商可對該品質系統下生產的所有產品發布符合性聲明，不必對每個個別產品型式重複公告機構審查。

路徑的核心差異：

- 模組 B+C：聚焦產品。代表性產品型式會被測試與認證。
- 模組 H：聚焦流程。製造商的整體設計與生產系統會被認證與監督。

符合性評鑑路徑

A

模組

自我評鑑

預設產品，以及完整適用調和標準、共同規格或認證方案的重要 Class I 產品。製造商對設計與生產承擔完整責任。

B+C

模組

型式與生產

適用於沒有可適用標準的重要 Class I 產品，也作為重要 Class II 路徑的一部分。公告機構審查代表型式；製造商確保每個生產單位符合。

H

模組

完整品質保證

可用於重要 Class I 與 II。公告機構端到端核准並稽核製造商的設計、開發、生產、測試與漏洞處理系統。

上市流程

技術文件

附件 VII 文件

→

EU 符合性聲明

附件 V 聲明已簽署

CE 標章已標示

標章已貼附於產品

→

上架產品

已投放 EU 市場

CRA 在 EU 法規架構中的定位

CRA 並非單獨存在。對製造商而言，實務問題是：CRA 工作在哪些其他 EU 法規下可以重複使用，又在哪些情況下仍須維持各自並行的義務？

CRA 工作可重複使用的場景

- **高風險 AI 系統（AI Act，規則 2024/1689）。** 如果產品是落在 CRA 範圍內的高風險 AI 系統，符合 CRA 基本資安要求即視為在 EU 符合性聲明所涵蓋範圍內，滿足 AI Act 的資安要求。原則上符合性評鑑程序透過 AI Act 體系進行，重要與關鍵 CRA 產品另有例外。CRA 資安風險評估必須納入 AI 特有風險，例如資料中毒與對抗式攻擊。
- **與其他 EU 法整合的風險評估。** CRA 明確允許資安風險評估構成另一 EU 法律規範下更廣泛風險評估的一部分，前提是產品同時落入兩個體系。一份評估產出，可作兩種法規用途。
- **單一技術檔案涵蓋多個體系。** 如同前述技術檔案章節所述，單一整合技術檔案可同時涵蓋 CRA 與其他適用 EU 法規，前提是各體系義務都已處理。對於已需依無線電設備指令、永續產品生態設計規則或其他產品法規提供文件的相同產品，這是有用的安排。
- **翻新、維護與維修的共用定義。** CRA 從永續產品生態設計規則匯入這些定義。在分析某項服務作業是否構成實質修改時，參考依據是 ESPR 的定義，而非 CRA 特有用語。

仍須維持獨立義務的場景

- **AI Act 其他事項。** 資安只是 AI Act 的其中一部分。風險分類、透明度、資料集治理、人為監督、AI 行為的上市後監控等，是 AI Act 的義務，CRA 並未處理。符合 CRA 的資安並不等於整體符合 AI Act。
- **生態設計與數位產品護照內容。** 生態設計關於能源效率、耐用度、可維修性評分，以及數位產品護照的永續性內容要求，並非 CRA 範圍。CRA 證據鏈可與生態設計工作並列，但無法取代。
- **資料法的 IoT 資料存取權。** 資料法賦予使用者對連網產品所產生資料的存取、分享與移轉契約權利。CRA 涵蓋該資料的安全；它並未設定存取權利制度。義務不同，證據也不同。
- **缺陷產品的產品責任。** 產品責任指令（2024/2853）對於缺陷產品所造成損害，仍課製造商以無過失責任。CRA 指出，欠缺上市後安全更新可能構成觸發責任的缺陷。你的合約、保險與事件應對手冊，必須與 CRA 符合性分開考量此風險暴露。

CRA Evidence 的顧問服務

CRA Evidence 將 EU 網路韌性法案義務轉換成可驗證的產品證據，並結合合規平台與技術顧問服務。

平台

集中管理 CRA 準備度背後的證據。

- **SBOM 與元件清單：** 針對產品版本與發布的 CycloneDX、SPDX、HBOM 記錄
- **CI/CD 證據自動化：** 掃描、SBOM 上傳、發布閘門與稽核記錄的 CLI/API 工作流程
- **簽章 SBOM 與來源：** 版本化證據、供應商證明與盡職調查記錄
- **漏洞運作：** CISA KEV、EPSS、VEX、監控、分流與通報工作流程
- **技術檔案與 CE 證據：** EU 聲明記錄、保存歷史與 QR 連結產品合規護照

技術顧問

協助將 CRA 義務轉換成產品、架構、發布流程與供應商模型的工程決策。

- **技術準備衝刺：** 基本要求差距檢視、架構建議與優先行動計畫
- **CRA 專案負責人：** 責任模型、義務追蹤、證據里程碑與技術檔案維護
- **主管機關與事件應變計畫：** 通報工作流程、詢問應對手冊、使用者溝通與證據包準備
- **法規對齊：** 將 CRA 證據連結到 Data Act、ESPR、AI Act、RED 與產業要求
- **技術工作坊：** 與產品、工程、資安、合規及供應商團隊進行遠端或現場會議

不綁定工具：CRA Evidence 可整合 CycloneDX、SPDX、Grype、Trivy、CI/CD 流程與議題追蹤系統。

實務上的第一步

選擇一個產品系列。整理負責人、適用範圍決策、SBOM、漏洞工作流程、技術檔案缺口與發布證據。這能建立具體的 CRA 基準，而不是把合規變成另一個獨立專案。

CRA Evidence 的完整支援範圍可於 craevidence.com/zh-tw 查閱。45 分鐘免費諮詢可於 craevidence.com/zh-tw/assessment 預約。