# 欧盟 CRA（网络弹性法案）快速自查清单

## 智能硬件 / IoT / 工业设备出口商实用版（2026）

**English title:** CRA Quick Compliance Self-Assessment Checklist for Chinese Exporters of Smart Hardware, IoT & Industrial Equipment (2026 Edition)

**关键时间线**

- **2026-09-11 报告义务开始适用**：CRA Article 14 关于被主动利用漏洞和严重事件的报告义务开始适用。
- **2027-12-11 CRA 主要义务全面适用**：CRA 主要义务全面适用，包括产品网络安全要求、技术文档、符合性评估等。

**一句话价值**：5 分钟快速判断您的产品是否已准备好应对欧盟客户问卷、合同责任与 2026 年 9 月报告义务。

编制：CivCom 法律审查团队（执业律师主导复核）

---

## 使用说明

请逐项勾选，并在“备注 / 现有证据位置”栏填写现有文件或缺失情况。建议由合规、法务、销售、研发、质量和供应链团队共同完成。

---

## 1. 为什么现在必须做这个检查

欧盟 CRA 是针对含数字元素产品（products with digital elements）的横向网络安全法规。对中国智能硬件、IoT、工业网关、机器人、自动化设备和其他联网产品出口商而言，风险不只来自监管本身，还来自欧洲客户提前传导的问卷、采购附件、SBOM 请求、漏洞报告义务、软件更新承诺和合同赔偿条款。

最容易被低估的是：客户文件中的一句确认，可能在后续订单、召回、审计、违约和索赔中成为证据。因此，CRA 准备工作应当同时连接 **产品事实、技术证据、客户文件和合同责任边界**。

---

## 2. 核心自查清单（共 36 项）

### 模块 1：适用性与产品分类判断

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 1 | 产品是否属于“含数字元素的产品”（Products with Digital Elements），即能直接或间接连接网络的硬件或软件? | ☐ | ☐ | ☐ | | 合规/法务/产品 |
| 2 | 产品是否支持远程更新、数据收集、远程访问或无线通信? | ☐ | ☐ | ☐ | | 研发/产品/合规 |
| 3 | 产品是否属于重要产品（Important Products）Class I 或 Class II，或关键产品（Critical Products）？ | ☐ | ☐ | ☐ | | 合规/认证/法务 |
| 4 | 贵公司是否为非欧盟制造商？是否已在欧盟指定授权代表（Authorized Representative）？ | ☐ | ☐ | ☐ | | 法务/销售/管理层 |
| 5 | 产品当前是否已加贴 CE 标志？是否计划在 2027 年 12 月 11 日后继续出口欧盟? | ☐ | ☐ | ☐ | | 认证/销售/管理层 |

### 模块 2：基本网络安全要求（Essential Cybersecurity Requirements）

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 6 | 是否已针对产品进行正式的网络安全风险评估（包括合理可预见误用场景）？ | ☐ | ☐ | ☐ | | 研发/信息安全/合规 |
| 7 | 产品是否实现“默认安全”（Security by Default），即开箱即用无需额外配置即具备基本安全? | ☐ | ☐ | ☐ | | 研发/产品 |

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 8 | 是否已消除产品中已知的可被主动利用的漏洞? | ☐ | ☐ | ☐ | | 研发/信息安全 |
| 9 | 是否建立机制确保在产品整个支持周期内提供安全更新? | ☐ | ☐ | ☐ | | 研发/售后/合规 |
| 10 | 是否明确定义并公开产品支持周期（建议至少 5 年）？ | ☐ | ☐ | ☐ | | 产品/法务/销售 |
| 11 | 是否实施安全启动（Secure Boot）、安全更新机制和访问控制? | ☐ | ☐ | ☐ | | 研发/信息安全 |
| 12 | 是否对产品进行过渗透测试或安全评估? | ☐ | ☐ | ☐ | | 研发/测试/合规 |
| 13 | 是否有机制及时接收和处理第三方报告的漏洞? | ☐ | ☐ | ☐ | | 信息安全/法务/客服 |

### 模块 3：技术文档与符合性评估

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 14 | 是否已准备符合 Annex II 要求的技术文档（包括产品描述、安全特性、风险评估、测试报告等）？ | ☐ | ☐ | ☐ | | 认证/研发/合规 |
| 15 | 是否已生成机器可读的 SBOM（Software Bill of Materials，软件物料清单）？ | ☐ | ☐ | ☐ | | 研发/信息安全 |
| 16 | 是否明确产品符合性评估路径（自我声明还是需第三方机构评估）？ | ☐ | ☐ | ☐ | | 认证/合规/法务 |

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 17 | 技术文档是否包含漏洞管理政策和协调漏洞披露（CVD）流程? | ☐ | ☐ | ☐ | | 信息安全/法务/合规 |
| 18 | 是否有内部流程确保技术文档持续更新? | ☐ | ☐ | ☐ | | 合规/研发/质量 |
| 19 | 是否已指定负责符合性评估的内部责任人或团队? | ☐ | ☐ | ☐ | | 管理层/合规 |

## 模块 4：漏洞与事件报告义务（2026 年 9 月 11 日起重点）

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 20 | 是否建立 24 小时内向 ENISA 和国家 CSIRT 报告被主动利用漏洞的流程? | ☐ | ☐ | ☐ | | 信息安全/法务/管理层 |
| 21 | 是否有机制在发现严重安全事件后 24 小时内报告? | ☐ | ☐ | ☐ | | 信息安全/法务 |
| 22 | 是否已准备好漏洞披露政策并公开联系点? | ☐ | ☐ | ☐ | | 信息安全/客服/法务 |
| 23 | 内部是否明确漏洞报告和事件响应的责任分工和升级流程? | ☐ | ☐ | ☐ | | 管理层/信息安全/法务 |
| 24 | 是否有工具或流程跟踪和记录所有已知漏洞及修复状态? | ☐ | ☐ | ☐ | | 信息安全/研发 |

## 模块 5：合同与责任边界

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 25 | 欧盟客户问卷或采购合同中是否包含高风险条款（如无限产品责任、24 小时报告义务、SBOM 强制披露、无限召回赔偿等）？ | ☐ | ☐ | ☐ | | 法务/销售/合规 |
| 26 | 是否已在现有或拟签订的合同中合理分配漏洞更新、事件报告、产品责任和召回成本? | ☐ | ☐ | ☐ | | 法务/销售/管理层 |
| 27 | 是否已识别合同中要求超出当前技术能力或证据范围的承诺? | ☐ | ☐ | ☐ | | 法务/研发/质量 |
| 28 | 是否准备好针对欧盟客户问卷的英文回复模板和红线修改建议? | ☐ | ☐ | ☐ | | 法务/销售 |
| 29 | 现有测试报告、认证、质量文件能否直接用于支撑合同中的合规承诺? | ☐ | ☐ | ☐ | | 质量/认证/法务 |
| 30 | 是否已建立跨部门（销售-法务-研发-质量）证据缺口确认机制? | ☐ | ☐ | ☐ | | 管理层/法务/合规 |
| 31 | 合同中是否包含合理的“已知信息范围”和“合理努力”限制条款? | ☐ | ☐ | ☐ | | 法务/销售 |

## 模块 6：供应链与证据准备

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 32 | 是否对第三方组件和开源软件进行过安全与许可尽职调查? | ☐ | ☐ | ☐ | | 研发/法务/采购 |
| 33 | 是否要求供应商提供机器可读 SBOM 和漏洞披露承诺? | ☐ | ☐ | ☐ | | 采购/研发/法务 |

| 编号 | 检查项 | 是 | 否 | 部分 | 备注 / 现有证据位置 | 责任部门 |
|---|---|---|---|---|---|---|
| 34 | 现有 CE 技术文件、测试报告能否映射到 CRA 证据要求? | ☐ | ☐ | ☐ | | 认证/质量/合规 |
| 35 | 是否有流程确保供应链变更时同步更新 SBOM 和技术文档? | ☐ | ☐ | ☐ | | 采购/研发/质量 |
| 36 | 中国侧网络安全标签制度要求是否已同步评估? | ☐ | ☐ | ☐ | | 合规/法务/产品 |

---

## 3. 自评结果与行动优先级

每项“是”记 1 分，总分 36 分。若某项为“部分”，建议先不计分，并在备注栏列出需要补充的证据、责任部门和完成时间。

| 分数 | 颜色 | 判断 | 建议行动 |
|---|---|---|---|
| 30 分以上 | 绿色 | 基础准备较好 | 继续维护证据台账，并对客户文件做逐项留痕 |
| 20-29 分 | 黄色 | 存在明显缺口 | 3 个月内优先补齐 SBOM、漏洞流程、更新政策、技术文档和合同回复口径 |
| 20 分以下 | 红色 | 高风险 | 不建议直接确认客户问卷，应先做文件审查、证据缺口 Memo 和责任边界评估 |

### 客户常见高风险条款 Top 10

1. **SBOM disclosure**：可能泄露第三方组件、开源组件、版本信息和安全敏感资料。

初步处理方向：限定披露范围、保密条件、合理请求、格式、用途和接收方。

1. **24-hour vulnerability reporting**：“any vulnerability”过宽，24 小时可能不现实，且未区分已确认漏洞和疑似问题。

初步处理方向：改为重大、已确认、影响产品安全的漏洞；设置初步通知和后续更新机制。

1. **Unlimited product safety indemnity**：把监管罚款、召回、第三方索赔无限转嫁给供应商。

初步处理方向：限定为供应商违约或缺陷导致、可归责范围、合理费用和责任上限。

1. **All applicable EU laws warranty**：过度概括，可能覆盖供应商无法判断或无法控制的进口商、平台、销售地义务。

初步处理方向：限定到供应商产品、技术文件和自身控制范围；区分进口商/经销商义务。

1. **No Russia / sanctions flow-down**：要求供应商保证下游和终端流向，可能超过其控制范围。

初步处理方向：改为合理努力、已知客户范围、直接交易方承诺和异常通知机制。

1. **Forced labour declaration**：把全部供应链绝对保证压给供应商，超出可核查范围。

初步处理方向：改为政策、尽调程序、已知范围、风险缓解和配合审计。

---

## 4. 下一步行动

- 免费阶段：完成本清单，确认产品范围、客户文件类型、证据缺口和内部责任人。
- 模板阶段：准备高风险合同条款回复模板、证据台账模板和英文客户回复口径。
- 专项审查服务：对客户问卷、采购附件、SBOM 请求、漏洞报告条款和赔偿责任做逐项审查。

联系入口：https://civcom.org/contact/

资料提交通知：https://civcom.org/privacy-intake-notice/

网站：https://civcom.org/free-cra-checklist/

---

## 5. 中英双语关键术语对照表

| 中文 | English | 简要说明 |
| --- | --- | --- |
| 网络弹性法案 | Cyber Resilience Act (CRA) | 欧盟网络安全核心法规 |
| 含数字元素的产品 | Products with Digital Elements | CRA 适用范围 |
| 软件物料清单 | Software Bill of Materials (SBOM) | 机器可读的软件、组件和依赖清单 |
| 协调漏洞披露 | Coordinated Vulnerability Disclosure (CVD) | 漏洞接收、确认、修复和公开政策 |
| 重要产品 | Important Products | Class I / Class II 分类 |

| 中文 | English | 简要说明 |
| --- | --- | --- |
| 关键产品 | Critical Products | 通常涉及更高符合性评估要求 |
| 欧盟授权代表 | Authorized Representative | 非欧盟制造商的欧盟责任安排之一 |
| 技术文档 | Technical Documentation | Annex II 相关证明材料 |
| 漏洞报告义务 | Vulnerability Reporting Obligation | 2026 年 9 月 11 日起适用的重点义务 |
| 产品责任 | Product Liability | 客户合同和欧盟产品责任规则共同影响的风险 |
| 召回责任 | Recall Responsibility | 采购合同中常见高风险责任项 |
| 默认安全 | Security by Default | CRA 基本网络安全要求之一 |
| 安全更新支持期 | Security Update Support Period | 需与产品支持周期、客户承诺和合同责任衔接 |

---

## 6. 免责声明与版权

本材料用于一般信息、内部首轮判断和业务沟通，不构成正式法律意见，也不建立律师—客户关系。具体事项应基于完整客户文件、产品事实、技术证据、交易安排和适用法律另行判断。本材料由 CivCom 编制，欢迎转发，但请注明来源。