

Commission Implementing Regulation (EU) 2025/2392 对照标准一览

Commission Implementing Regulation (EU) 2025/2392 已于 2025 年 12 月 1 日刊登欧盟官方公报，2025 年 12 月 21 日生效。本实施法案依《网络韧性法》CRA, Regulation (EU) 2024/2847 第 7(4) 条授权订定，为 CRA Annex III「重要产品」与 Annex IV「关键产品」的每一个类别给出具法律拘束力的技术描述，共 26 类。

分级直接决定产品适用哪些标准与符合性评鉴的深度，是输欧厂商 CRA 项目的第一份必读文件。以下整理判定原则、26 类分级与对应标准，并说明「分级」与「应符合的标准数量」为何是两件事。

一、分类判定原则

1. 核心功能是唯一判准 (Recital 2)：决定产品归属的是核心功能，而非规格列表。起点永远是「这个产品是什么」，不是「它能做什么」。
2. 组件不向上传染，但组件安全责任向上传 (Recital 3)：整合 embedded browser 的新闻 App 不因此变成浏览器类产品；只有产品整体构成重要或关键产品时才适用该分级。但技术文件仍须评估所整合组件的安全性。
3. 附加功能不使产品脱离其类别 (Recital 4)：路由器整合防火墙、操作系统内含计算器，皆不影响其原有分级。
4. 「有能力执行」不等于「核心功能」(Recital 5)：SOAR 有能力执行 SIEM 功能但核心功能不同，一般不属 SIEM；智能型手机虽整合 OS 与密码管理器，官方明示一般属 default tier。
5. 无论分级，风险评鉴一律要做 (Recital 6)：所有制造商依 CRA Article 13(2)、(3) 都须执行完整风险评鉴。分级决定的是评鉴路径，不是要不要做。
6. 例示清单不具穷尽性 (Recital 7)：附件中所有「includes but is not limited to」皆为开放式，产品不在例示中不等于不在范围内。

此外，Recital 8 引入本规则唯一的量化门坎：以 Common Criteria 的 AVA_VAN 等级区分芯片类产品——未设门坎者为 Class I，AVA_VAN 2 或 3 为 Class II，至少 AVA_VAN.4 为 Critical。

二、26 类产品分级与对应标准

以下对照 M/606 标准化授权下 ETSI、CEN、CENELEC 三方目前的标准编号。多数标准仍在制定中，编号与内容可能变动。

Annex I / Class I — 重要产品第一类（19 类）

#	产品类别	判定要点	对应标准
1	身分管理与特权存取管理 (IdM / PAM)	提供认证或授权机制 ;含控制存取数字资源或实体场所之系统 ; 含认证与门禁读取器、生物特征读取器	EN 40000-10 (CEN)
2	独立式与嵌入式浏览器	具 browser engine、支持 HTTP/HTTPS、可执行 script 与管理 cookies。明文涵盖具 AI agent 整合的浏览器	EN 304 617
3	密码管理器	本机或远程储存密码, 含产生、分享与应用整合	EN 304 618
4	恶意软件搜寻 / 移除 / 隔离软件	即 antivirus / antimalware	EN 304 619
5	VPN 功能产品	建构加密逻辑信道 ; 含 client / server / gateway	EN 304 620 / EN 50770-4 (OT)
6	网络管理系统	监控并控制连网组件之运作与组态 ; 含 SDN controller	EN 304 621 / EN 50770-2 (OT)
7	SIEM 系统	多来源搜集、分析关联, 以可行动信息呈现供资安用途	EN 304 622 / EN 50770-6 (OT)
8	开机管理程序	管理开机初始化与 OS 加载 ; 含 UEFI firmware、boot loader	EN 304 623
9	PKI 与数字证书签发软件	凭证之签发、更新、撤销及相关密钥管理	EN 304 624
10	实体与虚拟网络接口	有线 / 无线 NIC、控制器、转接器 (Wi-Fi、Ethernet、	EN 304 625 / EN 50770-3

#	产品类别	判定要点	对应标准
		USB、Bluetooth、NearLink、Zigbee、Fieldbus 等) 含 vNIC、CNI、VPN interface	(OT)
11	操作系统	提供硬件抽象接口并控制软件执行；含 RTOS	EN 304 626
12	路由器、连网用调制解调器、交换器	Switch 须具管理平面；无线基地台（AP）明列于 bridge 例示中	EN 304 627 / EN 50770-5 (OT)
13	具安全功能之微处理器	额外提供加密、认证、安全密钥储存、TEE 等，目的在保护自身以外之产品、网络或服务	EN 50765
14	具安全功能之微控制器	同上，惟为内建内存之可程序化 IC	EN 50765
15	具安全功能之 ASIC 与 FPGA	客制设计或可重新程序化 IC，额外具备前述安全功能	EN 50765
16	智慧家庭通用虚拟助理	于公共因特网通讯，处理自然语言提示并控制住宅连网装置	EN 304 631
17	具安全功能之智能家居产品	保护住宅中消费者人身安全且可远程控管；含智能门锁、婴儿监视、警报系统、家用摄影机	EN 304 632
18	具社交互动或定位追踪功能之连网玩具	受 2009/48/EC 规范。仅侦测邻近性（proximity）者不视为具定位追踪功能	EN 304 633
19	健康监测 / 儿童用穿戴式产品	健康监测型排除落入 MDR 2017/745 与 IVDR 2017/746 者；儿童型指供未满 14 岁者穿戴	EN 304 634

Annex I / Class II — 重要产品第二类 (4 类)

#	产品类别	判定要点	对应标准
1	Hypervisor 与 container runtime	含 type 1 / type 2 / hybrid 及巢状虚拟化	EN 304 635
2	防火墙、入侵检测与防御系统	含 network 与 application firewall (WAF、anti-spam gateway)、IDS、IPS	EN 304 636 / EN 50770-1 (OT)
3	防篡改微处理器	Class I #13 且具 tamper 防护, 设计达 AVA_VAN 2 或 3	EN 50766
4	防篡改微控制器	Class I #14 且具 tamper 防护, 设计达 AVA_VAN 2 或 3	EN 50766

Annex II — 关键产品 (3 类)

#	产品类别	判定要点	对应标准
1	具 Security Box 之硬件装置	由多个离散组件组成并具 tamper 实体封装 ;含实体支付终端机、HSM、行车纪录器	CEN/TC 224 工作项目 (编号未定)
2	智能电表网关及其他进阶安全用途装置	依 Directive (EU) 2019/944 Art. 2(23) ; 支持加解密、内含防火墙功能并可控制其他装置	CEN-CLC/JTC 13 WG 6 工作项目 (编号未定)
3	智能卡或类似装置, 含 secure element	设计达至少 AVA_VAN.4 ;含 TPM、eUICC、身分与旅行证件、实体支付卡、门禁卡	EN 50764 (硬件层) + EN 18330 (应用层)

横向标准（所有产品皆适用，不分级别）

标准	内容
EN 40000-1-1	名词与定义
EN 40000-1-2	网络韧性原则与风险管理（对应 Annex I Part I）
EN 40000-1-3	弱点处理（对应 Annex I Part II）
EN 40000-1-4	通用安全要求（建构于 EN 18031 系列并加以扩充）

三、分级只有一个，适用标准可能有很多份

分级由产品整体的核心功能决定，只有一个；技术文件中必须左证的标准数量，取决于产品实际具备多少项具实质重要性的功能。

Recital 4 明示产品整合另一类别的功能不影响其原有分级——但这只解决归属问题，并未免除该功能的技术要求。制造商依 Article 13 仍须就产品整体执行风险评鉴，一旦识别出该功能面的威胁，对应控制措施就必须落实并左证。

以一台企业级无线路由器为例——分级：核心功能为 router → Annex III Class I #12。应对照的标准：

- 横向：EN 40000-1-2、EN 40000-1-3（无条件适用）
- 主要垂直：EN 304 627
- 整合防火墙功能：EN 304 636 相关控件
- 提供 VPN server：EN 304 620 相关控件
- 具集中管理平台：EN 304 621 相关控件
- 自有操作系统：EN 304 626 相关控件
- 同型号销往工控 / OT 市场：另需对照 EN 50770-1 / -5 等 IEC 62443 基础的 OT profile
- 含 RF 功能：CRA 与 RED (EU) 2014/53 Art. 3(3)(d)(e)(f) 及 EN 18031 系列并行适用，须整并规划。

也就是说，这台产品分级只有一个，却可能需要对照六份以上的标准文件。反向情境同样要注意：若复合功能重到让产品整体的核心功能实质上变成次世代防火墙 / UTM 而非路由器，则整机分级直接由 Class I 升为 Class II。分级判错，错的是整条符合性评鉴程序；功能盘点漏掉，缺的是技术文件里的左证——两者都会在审查阶段被退回。

欢迎与世腾业务或法规团队联系，安排产品线的 CRA 分级盘点与标准对照。

本文所列标准编号与委员会分工依撰稿时公开信息整理，多数标准仍在制定中，内容与编号可能变动。本文仅供信息参考，以法规与公告单位宣告为准。