CRA checklist for Annex I, Art. 13 and Art. 14

> **Note**
> One row per requirement, to assess per product and product version. Enter the status (open / partly / met / not applicable), your evidence from the technical documentation, the owner and a due date. Justify requirements that do not apply in the risk assessment.

Annex I – Essential cybersecurity requirements

Part I – Requirements relating to the properties of products with digital elements

No.	Requirement	What an audit wants to see	Status	Evidence / note
1	Appropriate level of cybersecurity based on the risks Annex I Part I No. 1	Evidence of the risk assessment (Art. 13(2), (3)) and a documented secure development process (e.g. based on IEC 62443-4-1): security requirements, threat modeling, secure coding, reviews, testing. The risk assessment must state how no. 1 is applied.		
2	Made available without known exploitable vulnerabilities Annex I Part I(2)(a)	Release gate with SBOM comparison against vulnerability databases; exploitability assessment for each finding (VEX); checking of stock before delivery. Evidence: scan reports and release approval record for each release.		
3	Secure default configuration and ability to reset Annex I Part I(2)(b)	Table of the default configuration (services, ports, accounts, default state) and evidence that no default passwords exist; factory reset test. Document deviations for customized products in the contract.		
4	Vulnerabilities addressed through security updates Annex I Part I(2)(c)	Update mechanism with signature verification; justify the decision on automatic updates (including opt-out, notification, postponement) in the risk assessment. Evidence: update concept and test report for the update path.		
5	Protection against unauthorized access and reporting of possible unauthorized access Annex I Part I(2)(d)	Roles and permissions concept, authentication (local/central), brute-force protection, logging of failed sign-ins. Evidence: design document, penetration test report on authentication and authorization.		
6	Confidentiality of stored, transmitted and otherwise processed data Annex I Part I(2)(e)	State-of-the-art encryption (e.g. TLS 1.2/1.3, encrypted storage of credentials and recipes), key storage in hardware. Evidence: cryptography concept referring to BSI TR-02102, configuration check.		
7	Integrity of data, commands, programs and configuration; reporting of corruption Annex I Part I(2)(f)	Secure boot, signed firmware and application programs, integrity checks of configurations, detection and reporting of tampering. Evidence: test with a manipulated image, log of the rejection.		

No.	Requirement	What an audit wants to see	Status	Evidence / note
8	Data minimization Annex I Part I(2)(g)	Data inventory: which data (personal and other), for what purpose, where to. Telemetry only to the extent necessary and configurable. Evidence: data flow analysis and configuration options.		
9	Availability of essential and basic functions, also after incidents and under DoS Annex I Part I(2)(h)	Definition of essential functions; rate limiting, prioritization of real-time traffic, safe state under overload. Evidence: robustness and load test reports (e.g. network stress tests, fuzzing).		
10	Minimizing negative impact on other devices and networks Annex I Part I(2)(i)	Limiting of broadcast/multicast and reconnection attempts, no unfiltered bridging between networks, remote maintenance only under control. Evidence: architecture assessment and network tests.		
11	Limiting attack surfaces, including external interfaces Annex I Part I(2)(j)	Interface inventory with a justification for each open interface; debug interfaces (JTAG/UART) disabled or protected in series production; minimal OS image. Evidence: port scan, hardware review.		
12	Reducing the impact of incidents through exploitation mitigation mechanisms Annex I Part I(2)(k)	Compiler hardening (stack protection, ASLR, NX), least privilege for processes, sandboxing, separation of safety-critical functions. Evidence: build configuration, hardening check (e.g. checksec).		
13	Security-related logging/monitoring with opt-out Annex I Part I(2)(l)	Security log for sign-ins and changes to configuration, programs and firmware; export (syslog); document the opt-out option. Evidence: logging concept and sample logs.		
14	Permanent secure deletion and secure transfer of data and settings Annex I Part I(2)(m)	Factory reset or deletion function for all data, accounts, certificates and keys; secure export/import function for configurations. Evidence: forensic deletion test, instructions in the user information (Annex II no. 8(d)).		

Part II – Vulnerability handling requirements

No.	Requirement	What an audit wants to see	Status	Evidence / note
15	Identifying and documenting vulnerabilities and components, software bill of materials Annex I Part II No. 1	SBOM in a machine-readable format (CycloneDX/SPDX) covering at least the top-level dependencies for each release; continuous monitoring. Evidence: SBOM concept, SBOM register, monitoring logs.		
16	Addressing and remediating vulnerabilities without delay; security updates separate from functional updates Annex I Part II No. 2	Documented PSIRT process with response targets, maintenance branches and stand-alone security updates. Evidence: procedure, ticket history with timestamps.		
17	Regular and effective security tests and reviews Annex I Part II No. 3	Test plan with SAST, dependency scans, fuzzing, penetration tests and their frequency. Evidence: test reports in the technical documentation (Annex VII no. 6).		

No.	Requirement	What an audit wants to see	Status	Evidence / note
18	Publishing information on fixed vulnerabilities Annex I Part II No. 4	Security advisories (e.g. CSAF 2.0) with description, affected products/versions, impact, severity and remedial measures; criteria for justified postponement. Evidence: published advisories, approval process.		
19	Coordinated vulnerability disclosure (CVD) policy Annex I Part II No. 5	Public CVD policy with reporting channel, commitments, timeframes and safe harbor. Evidence: published policy (screenshot/URL), reference in the user information (Annex II no. 2).		
20	Facilitating the sharing of vulnerability information, providing a contact address Annex I Part II No. 6	Functional mailbox with PGP, web form, security.txt; channels to suppliers and coordinating bodies (e.g. CERT@VDE). Evidence: contact details on the website and in the product documentation.		
21	Mechanisms for the secure distribution of updates Annex I Part II No. 7	Signed packages, authenticated download channel, integrity check before installation, automatic distribution where appropriate; offline path for air-gapped plants. Evidence: update concept and test of the signature verification.		
22	Distributing security updates without delay and free of charge, with advice Annex I Part II No. 8	Rule on free-of-charge provision (exceptions only by contract, for customized products for business users); release notes with recommended actions. Evidence: update policy, sample release notes.		

Obligations of manufacturers and reporting obligations (Art. 13 and 14)

Obligations of manufacturers (Art. 13)

No.	Requirement	What an audit wants to see	Status	Evidence / note
23	Assess, document and keep the cybersecurity risks up to date Art. 13 Abs. 2, 3, 4 und 7	The risk assessment accompanies the product from planning through development, production and delivery to maintenance. It starts from the intended purpose, foreseeable use, operating environment and expected lifetime, states which requirements of Annex I Part I point 2 apply and how they are implemented, and is updated during the support period as soon as new vulnerabilities or third-party information become known. Evidence: an approved, versioned risk assessment in the technical documentation with a justification for every requirement that does not apply, and a change log.		
24	Due diligence for third-party components, including open source Art. 13(5)	Before a purchased or freely available component goes into the product, a check confirms whether it could endanger the product's cybersecurity: origin, maintenance state, known vulnerabilities, support commitments and license. This expressly also applies to open-source software that was not made available in the course of a commercial activity. Evidence: selection criteria for components, check records per component, supplier assessment and controlled inclusion in the build.		

No.	Requirement	What an audit wants to see	Status	Evidence / note
25	Report vulnerabilities in components to their manufacturer or maintainer and share fixes Art. 13(6)	If your own team finds a vulnerability in a built-in component, including an open-source component, it is reported to whoever produces or maintains the component and handled in your own product like any other vulnerability under Annex I Part II. If you developed a fix yourself, the code or the documentation goes back to that party, in machine-readable form where useful. Evidence: reporting channel per component, log of reports to upstream projects and suppliers, reference to the internal vulnerability case.		
26	Set and state the support period and handle vulnerabilities effectively within it Art. 13 Abs. 8 und 19	The support period follows the expected time of use and the reasonable expectations of users and is, as a rule, at least five years, or correspondingly shorter if the product is expected to be in use for less time. The reasons for the decision are recorded in the technical documentation. At the time of purchase the end date is clearly visible, stating at least month and year, and where technically feasible users receive a notification when the period ends. During the period, vulnerabilities are handled under Annex I Part II, based on a policy for coordinated vulnerability disclosure. Evidence: documented decision with reasons, statement on the product, packaging or website, vulnerability process with CVD policy.		
27	Keep security updates that were made available for at least ten years Art. 13 para. 9	Every security update made available to users during the support period stays available for at least ten years from its release, or longer if the support period runs longer. This includes a permanent update archive, secured signing keys and checksums, and a plan for changes of download platforms. Evidence: archive concept with retention period, list of released updates with dates, spot check that they can be retrieved.		
28	Retain the technical documentation and the EU declaration of conformity Art. 13(13)	The technical documentation and the EU declaration of conformity are kept for at least ten years after placing on the market, or for the support period if that is longer, and are presented to the market surveillance authority on request. Retention covers every version per product release, stays readable across system changes and is protected against modification. Evidence: storage location and retention rule, list of documentation versions per product, access concept.		
29	Provide and keep available information and instructions for users Art. 13 para. 18	The product comes with the information listed in Annex II, on paper or electronically, in a language easily understood by users and authorities, clear and legible, so that installation, operation and use are secure. The information stays available for at least ten years after placing on the market or for the longer support period; versions published online are accessible and user-friendly. Evidence: user information per product version checked against Annex II, language versions, place of publication and retention rule.		

Reporting obligations of manufacturers (Art. 14)

No.	Requirement	What an audit wants to see	Status	Evidence / note
30	Report actively exploited vulnerabilities on time (24 hours, 72 hours, 14 days) Art. 14 Abs. 1, 2 und 7	When the manufacturer becomes aware of an actively exploited vulnerability in the product, it reports it through ENISA's single reporting platform simultaneously to the competent coordinating CSIRT and to ENISA: an early warning within 24 hours naming the Member States concerned, a vulnerability notification within 72 hours with information on the product, the nature of the exploitation and countermeasures, and a final report no later than 14 days after a corrective or mitigating measure is available. The competent CSIRT is the one of the Member State of the main establishment. Evidence: reporting process with roles and deputies, access to the reporting platform, templates for the three stages, records of exercises or real reports.		
31	Report severe incidents affecting the security of the product (24 hours, 72 hours, one month) Art. 14 Abs. 3, 4 und 5	An incident is severe if it negatively affects, or is capable of affecting, the product's ability to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions, or if it has led or is capable of leading to the introduction or execution of malicious code in the product or in the user's systems. In that case the following go simultaneously to the CSIRT and ENISA through the single reporting platform: an early warning within 24 hours stating whether unlawful or malicious acts are suspected, an incident notification within 72 hours with an initial assessment and countermeasures, and a final report within one month of that notification. Evidence: assessment criteria for the classification, procedure from detection to reporting, templates, exercise records.		
32	Inform affected users about the vulnerability or incident and possible countermeasures Art. 14 para. 8	After becoming aware of an actively exploited vulnerability or a severe incident, the affected users, and where appropriate all users, are informed, including about what they can do themselves to mitigate or remedy the risk, where useful in a structured, machine-readable format such as CSAF. If the manufacturer fails to inform them, the coordinating CSIRT may inform the users itself. Evidence: communication plan with channels and target groups, template for security notices, published advisories with dates.		

About this template

Template version 1.0-3d9492d0
Content as of 12 November 2026
Published by Made with Complass, https://complass.eu

Legal basis (as of): Verordnung (EU) 2024/2847, amtliche deutsche Fassung auf EUR-Lex mit den Berichtigungen ABl. L 2025/90555, ABl. L 2025/90828 und ABl. L 2026/90667 (modules/lawtexts, abgerufen am 06.10.2026), Durchführungsverordnung (EU) 2025/2392, Delegierte Verordnungen (EU) 2025/1535 und 2026/881, Art. 104 der Verordnung (EU) 2025/327 (EHDS), Richtlinie (EU) 2024/2853, BSI TR-03183-2 Version 2.1.0. Leitlinien der Kommission C(2026) 5252 vom 27.07.2026 (Abschnitte 3.2, 4, 5, 8.1, 9.1 und 9.3.1 am 12.11.2026 im Volltext abgeglichen).

This template is not legal advice. It does not replace checking which requirements apply to your company and does not guarantee any audit or certification result.

License: Creative Commons Attribution 4.0 International (CC BY 4.0). You may use, change and pass on the template, also commercially, as long as you name the source. Attribution: "Template: Complass (complass.eu), CC BY 4.0". https://creativecommons.org/licenses/by/4.0/deed.en