Raspberry Pi and the European Cyber Resilience Act (CRA)

Colophon

© 2022-2026 Raspberry Pi Ltd

This documentation is licensed under a Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND).

Release	3
Build date	26/10/2026
Build version	644fcd2ec60f

Legal disclaimer notice

TECHNICAL AND RELIABILITY DATA FOR RASPBERRY PI PRODUCTS (INCLUDING DATASHEETS) AS MODIFIED FROM TIME TO TIME ("RESOURCES") ARE PROVIDED BY RASPBERRY PI LTD ("RPL") "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN NO EVENT SHALL RPL BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE RESOURCES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RPL reserves the right to make any enhancements, improvements, corrections or any other modifications to the RESOURCES or any products described in them at any time and without further notice.

The RESOURCES are intended for skilled users with suitable levels of design knowledge. Users are solely responsible for their selection and use of the RESOURCES and any application of the products described in them. User agrees to indemnify and hold RPL harmless against all liabilities, costs, damages or other losses arising out of their use of the RESOURCES.

RPL grants users permission to use the RESOURCES solely in conjunction with the Raspberry Pi products. All other use of the RESOURCES is prohibited. No licence is granted to any other RPL or other third party intellectual property right.

HIGH RISK ACTIVITIES. Raspberry Pi products are not designed, manufactured or intended for use in hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems or safety-critical applications (including life support systems and other medical devices), in which the failure of the products could lead directly to death, personal injury or severe physical or environmental damage ("High Risk Activities"). RPL specifically disclaims any express or implied warranty of fitness for High Risk Activities and accepts no liability for use or inclusions of Raspberry Pi products in High Risk Activities.

Raspberry Pi products are provided subject to RPL's Standard Terms. RPL's provision of the RESOURCES does not expand or otherwise modify RPL's Standard Terms including but not limited to the disclaimers and warranties expressed in them.

Document version history

Release	Date	Description
1	10 Jun 2026	Initial release
2	10 Sep 2026	Major update: corrected Act status and timeline; added product classifications, a fixed-vs-updatable deployment model, harmonised standards, relationships to other regulations, an expanded vulnerability-and-incident-reporting walkthrough, and updated tooling references (`rpi-image-gen`, `syft`, `grype`)
3	19 Oct 2026	Updated standards status and timelines; added Implementing Regulation (EU) 2025/2392, secure boot, and an expanded checklist; corrections

Scope of document

This document applies to the following Raspberry Pi products:

Single Board Computers / SBCs

Pi Zero			Pi Zero 2		Pi 1				Pi 2	Pi 3			Pi 4	Pi 5
-	W	H	W	WH	A	B	A+	B+	B	A+	B	B+	B	-
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Compute Modules

CM0	CM1	CM3	CM3+	CM4	CM4S	CM5
✓	✓	✓	✓	✓	✓	✓

Keyboard Computers

Pi 400	Pi 500	Pi 500+
✓	✓	✓

Contents

Introduction 5
What is the Cyber Resilience Act (CRA) and why choose Raspberry Pi? 5
Why Raspberry Pi is a strong platform for CRA compliance 5
How this document is organised 6
What is the CRA, and who is responsible? 7
The obligations of the manufacturer 7
What is excluded 7
Timelines 9
The legacy-product trap 9
Standardisation and guidance milestones 9
What the CRA requires of you 11
Product properties — Annex I Part I 11
Process requirements — Annex I Part II 12
The product support period 13
Support period and retention 13
Product classifications and conformity routes 14
Documentation and marking 15
Reporting obligations from 11 September 2026 16
Penalties 17
The current harmonised standards gap 18
Where the work stands 18
How this impacts the assessment of products by their product class 19
Planning without a presumption of conformity 19
Conducting the cybersecurity risk assessment 21
The CRA risk assessment requirements 21
Structuring the assessment: SP 800-30r1 mapped to the CRA 21
Choose and declare your scales 22
A short worked example 23
Documenting non-applicability 24
Turning an SBOM into a vulnerability list 24
Why choose Raspberry Pi? 25
Secure boot and the draft boot manager standard 26
Raspberry Pi OS and your monitoring 26
The Raspberry Pi support model 26
Raspberry Pi Connect 28
What is Raspberry Pi Connect? 28
Two update mechanisms 28
Mapping Raspberry Pi Connect capabilities to CRA requirements 29
Article 14 and the fourteen-day reporting window as a worked example 30
In summary: the operational case for Raspberry Pi Connect 31
What to do now 32
References 33
Contact us for more information 33

Introduction

What is the Cyber Resilience Act (CRA) and why choose Raspberry Pi?

Regulation (EU) 2024/2847 places binding cybersecurity requirements on manufacturers of connected products sold on the EU market. Integrators of Raspberry Pi computers who go on to place their products on the European market must ensure they comply with the CRA. This document sets out those obligations with references to the CRA, explains how to conduct a cybersecurity risk assessment, discusses the current state of the harmonised standards and the regulatory sphere, and maps the tools Raspberry Pi provides to support customers.

By the end of this document, it is hoped that the reader will have a clear understanding of the CRA obligations, the timelines for compliance, the steps required to ensure their products meet the requirements, and how the Raspberry Pi platform provides a low-friction route to conformity.

Why Raspberry Pi is a strong platform for CRA compliance

Choosing Raspberry Pi helps integrators easily meet the CRA requirements. While Raspberry Pi Ltd cannot discharge your obligations as a manufacturer, it has already built, tested, and maintained the infrastructure the CRA requires you to have, offering a mature platform to build upon. The infrastructure Raspberry Pi Ltd provides is the hardest to build from scratch; this includes a software bill of materials (SBOM), which is generated automatically for every software release; signed secure-boot and full-disk-encryption paths; automated updates and rollback; an update channel that reaches devices behind customer firewalls without opening a port; and a vulnerability disclosure process that is already in place.

As the integrator, you must still conduct the risk assessment and classification processes, choose your conformity route, and meet the reporting obligation should it be required. However, having this infrastructure in place ensures your own compliance effort can focus on factors that are genuinely specific to your products, rather than on re-inventing device identity, artefact integrity, and rollback from first principles.

Table 1.
Raspberry Pi is a strong platform for CRA compliance.

Raspberry Pi Ltd provides	Why it matters for the CRA
Published long-term hardware and software support commitments, with longevity data available on the Product Information Portal.	The CRA specifies that manufacturers must provide free security updates for a minimum of five years, while security updates and technical documentation must remain available for at least ten. In practice, this means choosing a compute platform you can commit to for as long as your product stays on the market. See What the CRA requires of you.
Automatic SBOM generation for every Raspberry Pi OS release and every `rpi-image-gen` build.	Annex I Part II(1) requires a machine-readable SBOM. Raspberry Pi already provides one for the platform layer without you having to build tooling of your own.
Signed secure boot and full-disk encryption with device-unique keys, provisioned at manufacture via `rpi-sb-provisioner`.	Directly evidences Annex I Part I(2)(d), (e), and (f) — protection from unauthorised access, confidentiality, and integrity.
A/B image updates with automatic rollback (`rpi-image-gen`), plus an outbound-only, firewall-friendly remote update channel (Raspberry Pi Connect).	The CRA's security fix delivery infrastructure and 14-day final report deadline are already in place in Raspberry Pi Ltd's existing infrastructure. See Raspberry Pi Connect.
Access to the upstream Debian security process for the majority of your software stack, plus Raspberry Pi Ltd's own advisories and coordinated disclosure policy.	Removes the need to build vulnerability-monitoring infrastructure for most of your software stack from scratch.

Raspberry Pi Ltd provides	Why it matters for the CRA
Documentation, application notes, and compliance guidance maintained by an internal CRA working group that tracks the regulation and the standardisation work.	Feeds directly into the technical documentation Annex VII requires.

Why choose Raspberry Pi? gives a tool-by-tool mapping of Raspberry Pi Ltd's existing infrastructure against specific CRA obligations.

Raspberry Pi Connect takes a deeper look at the update and reporting capabilities that support the publication of security patches, ensuring they are received by all deployed devices and that the reporting obligations are met.

How this document is organised

This is a long, reference-heavy document that maps a broad regulation onto product development decisions. It is intended to be consulted rather than read start to finish, and it mixes three kinds of material: legal obligations and timelines, an engineering methodology for the risk assessment, and a map of the Raspberry Pi tools that will help you meet the requirements. The table below is a guide to which section serves which need.

Table 2.
Document roadmap.

Section	Read this if you need to…
What is the CRA, and who is responsible?	…confirm whether the CRA applies to your product and who carries the obligation — you or Raspberry Pi Ltd.
Timelines	…work out what is due and when — including the reporting obligation that has applied since 11 September 2026, even to products already on the market.
What the CRA requires of you	…consult a comprehensive outline of the legislation, including essential requirements, documentation, support periods, product classifications, conformity routes, reports, and penalties.
The current harmonised standards gap	…understand why no presumption of conformity is available yet, and how to plan effectively without it.
Conducting the cybersecurity risk assessment	…write the risk assessment that gates every other requirement, with a worked methodology and example.
Why choose Raspberry Pi?	…see which CRA obligations Raspberry Pi Ltd's tooling already helps you meet, and where the responsibility remains yours.
Raspberry Pi Connect	…design the field update and reporting pipeline that Article 14's deadlines assume you have built.
What to do now	…read only one section — this distils the rest into a checklist.
References	…find the applicable source.

Note

Short on time? Read Introduction, Timelines, and What to do now, in that order. Everything else supports those three.

Note

Legal disclaimer: This document is provided for information purposes only and does not constitute legal advice. Classification of the product, determination of its support period, completion of the risk assessment, selection of a conformity route, and the content of the technical documentation are the responsibility of the manufacturer placing the product on the EU market. Seek legal advice where any requirement is unclear.

Technical and reliability data for Raspberry Pi products are provided "as is". Raspberry Pi Ltd reserves the right to make modifications to the resources described here.

What is the CRA, and who is responsible?

The Cyber Resilience Act — Regulation (EU) 2024/2847 — is the EU's horizontal cybersecurity regulation for hardware and software. It was adopted on 23 October 2024, published in the *Official Journal* of the European Union on 20 November 2024, and entered into force on 10 December 2024. It is a New Legislative Framework instrument: it works through essential requirements, a conformity assessment, a declaration of conformity, and CE marking — much the same as the Low Voltage Directive or the EMC Directive.

Its scope is deliberately wide. Article 3(1) defines a **product with digital elements** as a software or hardware product and its remote data processing solutions, including software or hardware components placed on the market separately. Article 2(1) brings in any such product whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. In practice, if your product digitally connects to anything and you sell it in the EU, assume it is in scope and conduct a cybersecurity risk assessment.

The obligations of the manufacturer

The CRA places substantive duties on the manufacturer of the finished product. Raspberry Pi Ltd's own compliance with respect to its boards, modules, and operating system is not transferable to your product, and the CE marking Raspberry Pi Ltd affixes to a computer does not discharge your obligations for the finished product it is integrated into.

For CRA purposes, you are the manufacturer if any of the following apply:

Table 3.
Becoming the manufacturer.

Circumstance	Reference
You place the product on the EU market under your own name or trademark	Article 3(13)
You are an importer or distributor who markets a product under your own name or trademark	Article 21
You make a substantial modification to a product already on the market and place the result on the market	Article 22

A change is **substantial** when it modifies the intended purpose in a way not foreseen in the initial risk assessment, or where the nature of the hazard has changed or the level of cybersecurity risk has increased. A security update that reduces risk is not a substantial modification; a feature update that broadens the attack surface generally is. Article 26 requires the Commission to issue guidance on changes; see Standardisation and guidance milestones for the current status.

Integrating Raspberry Pi hardware, customising the software stack, and shipping the result under your own brand makes you the manufacturer. Importers must verify manufacturer compliance before placing a product on the market (Article 19); distributors must verify CE marking and accompanying documentation (Article 20).

What is excluded

The CRA does not apply where the following EU law applies, as these regimes already address cybersecurity to an appropriate level:

Table 4.
Exclusions (Article 2(2) to (4)).

Regulation	Instrument	Reference
(EU) 2017/745	Medical devices	Article 2(2)(a)
(EU) 2017/746	In vitro diagnostic medical devices	Article 2(2)(b)
(EU) 2019/2144	Motor vehicle type approval	Article 2(2)(c)
(EU) 2018/1139	Products certified for civil aviation	Article 2(3)
Directive 2014/90/EU	Marine equipment	Article 2(4)

Also outside of scope: products developed or modified exclusively for national security or defence purposes; products specifically designed to process classified information (Article 2(7)); and identical spare parts that restore a product to its original function

(manufactured according to the same specifications as the components that they are intended to replace), (Article 2(6)). Free and open source software supplied outside the course of a commercial activity is not “made available on the market”.

If you use Raspberry Pi hardware and software in a product that is placed on the market, that product is not considered free or open source, and the manufacturer’s obligations under the CRA will apply. The good news is that Raspberry Pi provides tools and resources to make compliance as easy as possible.

Note

The single most consequential design decision: can your product receive authenticated software updates in the field? The CRA requires effective vulnerability handling for the whole support period, which is at least five years (Article 13(8)). A product with no field update mechanism can only satisfy that obligation if its intended lifetime is very short, or if a documented risk assessment justifies the absence of updates. If a CVE later lands in your software stack, your options narrow to user-actionable mitigation guidance, product recall, or non-compliance. This should be decided at the architecture stage, not the certification stage.

Timelines

The CRA is implemented in phases. Two dates are hard statutory deadlines that fall before full application, and now is the time to prepare for them. Any design work that is currently under way should be reviewed against the CRA requirements, and any products that are already on the market should undergo a cybersecurity risk assessment and be assessed for their vulnerability-handling and incident-response processes.

Table 5.
Key statutory dates.

Date	Event	Reference
20 Nov 2024	Published in the *Official Journal* (OJ L, 2024/2847).	–
10 Dec 2024	Came into force, 20 days after publication.	Article 71(1)
11 Jun 2026	Chapter IV applies. Member States may notify conformity assessment bodies, so notified bodies begin to become available.	Article 71(2)
11 Sep 2026	**Article 14 applies. Reporting of actively exploited vulnerabilities and severe incidents becomes mandatory, including for products already on the market.**	Article 71(2)
11 Dec 2027	Full Regulation applies: essential requirements, cybersecurity risk assessment, technical documentation, conformity assessment, EU declaration of conformity, and CE marking.	Article 71(2)

The legacy-product trap

Article 69(2) states that products placed on the market before 11 December 2027 become subject to the Regulation only if they are substantially modified after that date. That transitional relief does **not** extend to Article 14 (Article 69(3)). From 11 September 2026, reporting obligations apply to every in-scope product that has been made available on the EU market, including products you shipped years ago and have no intention of substantially modifying.

For most OEMs, this means the first CRA deliverable is not a declaration of conformity in 2027 — it is a working vulnerability-monitoring and incident-response process, covering the entire deployed fleet, by September 2026.

Standardisation and guidance milestones

These are not statutory deadlines, but rather current best guesses showing the timelines of available technical documents and standards.

Table 6.
Supporting ecosystem milestones.

Date	Event
Feb 2025	Commission presents standardisation request M/606 to CEN, CENELEC, and ETSI
3 Apr 2025	M/606 is formally accepted by all three European Standardisation Organisations; around 41 standards are requested
3 Dec 2025	Commission publishes its first FAQ document on CRA implementation (updated since)
27 Jul 2026	Commission approves its Article 26 guidance on applying the CRA (C(2026) 5252, approximately 80 pages)
30 Aug 2026	Mandate deadline for the horizontal type A standard and the type B standard for vulnerability handling
11 Sep 2026	ENISA Single Reporting Platform goes live for Article 14 notifications
1 Oct 2026	Formal vote closes on FprEN 40000-1-1 (vocabulary) and FprEN 40000-1-2 (principles and risk management); both reported as approved
30 Oct 2026	Mandate deadline for the product-specific type C standards

Date	Event
Nov 2026	EN 40000-1-1 and EN 40000-1-2 expected to be published
Jan 2027	prEN 40000-1-3 (vulnerability handling) expected to complete; ETSI EN 304 623 (boot managers) expected to be published
Apr 2027	Planned *Official Journal* citation of ETSI EN 304 623, the first firm citation date for any CRA standard
30 Oct 2027	Mandate deadline for the horizontal type B standards covering technical measures, including prEN 40000-1-4

Note

In early July 2026, the Commission published a draft amendment to M/606 that would postpone the 2026 mandate deadlines by two months: the type A and vulnerability-handling standards to **31 October 2026**, and the type C standards to **31 December 2026**. As at mid-October 2026, the amendment has not been adopted, so the dates in Table 6 remain the formal ones. The delay would not be enough in any case: the vulnerability-handling standard is not now expected before January 2027. Treat all of these dates as planning inputs rather than commitments. In all cases, such delays show that the Commission is aware of the practical difficulty of meeting the deadlines, and that it is willing to be flexible. The CRA itself does not provide for any delay in the statutory deadlines, so the 11 September 2026 reporting obligation remains firm.

The CRA represents a significant new field of regulation, and the entire market, from the Commission down, is still learning how to implement it. The Commission may have to be pragmatic in its enforcement of the CRA, taking into account the practical difficulties of compliance in the early years. However, the statutory deadlines are non-negotiable, and manufacturers must show that they are taking the CRA seriously and have a plan to meet the requirements.

What the CRA requires of you

For the purpose of clarity, it helps to group the requirements of the CRA. There is no legal basis for this, but it simplifies the discussion in this document.

Table 7.
Requirement groups under the CRA.

Obligation	Reference
Cybersecurity requirements relating to the properties of products	Annex I Part I (via Article 13(1))
Vulnerability-handling requirements	Annex I Part II (via Article 13(8))
Documentation and declaration requirements	Articles 28 to 32, and Annexes II, V, VII, and VIII
Reporting requirements	Article 14

Product properties — Annex I Part I

Point 1 of Annex I Part I is unconditional: the product must be designed, developed, and produced so as to ensure an appropriate level of cybersecurity based on the risks. Point 2 then lists 13 requirements that apply **on the basis of the cybersecurity risk assessment referred to in Article 13(2)**. That qualifier is very important — the risk assessment defines which of the essential requirements apply, and how. The Conducting the cybersecurity risk assessment section covers how to produce one.

The table below provides a list of the requirements and introduces the solutions Raspberry Pi makes available to the integrator. The solutions listed are discussed in more detail later in this document.

Table 8.
Annex I Part I requirements.

Requirement	Evidenced by	Reference	Raspberry Pi solution
No known exploitable vulnerabilities at the point of placement on the market.	SBOM, plus a dated vulnerability scan record for the shipped image.	Annex I Part I(2)(a)	`syft` and `grype`
Secure-by-default configuration, including the ability to reset to the original state.	Documented default configuration; factory-reset design; hardening rationale.	Annex I Part I(2)(b)	`rpi-image-gen` and `raspi-config`
Vulnerabilities addressable through security updates, with automatic updates enabled by default where applicable; plus, a clear opt-out mechanism, update notifications, and the option to postpone.	Update architecture description; A/B or equivalent scheme; opt-out mechanism.	Annex I Part I(2)(c)	`rpi-image-gen`, `raspi-config`, and `rpi-connect`
Protection from unauthorised access by appropriate control mechanisms, and reporting of possible unauthorised access.	Authentication design; no shared default credentials; access logging.	Annex I Part I(2)(d)	`rpi-image-gen` and `raspi-config`
Confidentiality of stored, transmitted, and processed data, such as by state-of-the-art encryption at rest or in transit.	Full-disk encryption configuration; TLS configuration and cipher policy.	Annex I Part I(2)(e)	`rpi-sb-provisioner` (full-disk encryption with device-unique keys).

Requirement	Evidenced by	Reference	Raspberry Pi solution
Integrity of data, commands, programs, and configurations against unauthorised modification; reporting of corruption.	Secure boot chain; signed packages; integrity monitoring.	Annex I Part I(2)(f)	`rpi-sb-provisioner` (secure boot, signed images) and Raspberry Pi Connect (per-artefact checksum verification).
Data minimisation — processing only the data that is adequate, relevant, and limited to the intended purpose.	Data-flow diagrams featuring a necessity rationale per data item.	Annex I Part I(2)(g)	Architecture decision — no Raspberry Pi tooling applies. Data-flow analysis is the integrator's responsibility.
Availability of essential and basic functions, including after an incident, with resilience and anti-denial-of-service measures.	Watchdog and recovery design; rate limiting; resource-exhaustion testing.	Annex I Part I(2)(h)	`rpi-image-gen` for A/B updates with automatic rollback, plus Raspberry Pi Connect. Many tools that support resilience and mitigate denial-of-service attacks — including watchdog timers and programs such as Traffic Control and Fail2Ban — can be implemented by the integrator.
Minimal negative impacts on the availability of services provided by other devices or networks.	Traffic behaviour testing; broadcast and multicast discipline.	Annex I Part I(2)(i)	Architecture decision — no Raspberry Pi tooling applies. Traffic behaviour testing is the integrator's responsibility.
Limited attack surfaces, including external interfaces.	Interface inventory with enabled/disabled state and justification.	Annex I Part I(2)(j)	`rpi-image-gen`, `raspi-config`, and Raspberry Pi OS Lite.
Impact of incidents reduced through appropriate exploitation mitigation mechanisms and techniques.	Compiler and kernel hardening flags; privilege separation; sandboxing.	Annex I Part I(2)(k)	`pi-gen-micro` (reduced functionality, minimised attack surface).
Provision of security-related information by recording and monitoring relevant internal activity, with a user opt-out mechanism.	Audit-log specification; retention and export design.	Annex I Part I(2)(l)	Audit log in Raspberry Pi Connect for Organisations can be used to monitor and record connections to deployed devices. From there, integrators can track updates.
Ability for users to securely and permanently remove all data and settings, and to transfer data securely where possible.	Secure erase procedure; destruction of encrypted volumes.	Annex I Part I(2)(m)	`OS image runtime` (crypto-erase via destruction of encrypted volume(s) LUKS header).

Where a requirement is not applicable to your product, Article 13(4) obligates you to include a clear justification in the technical documentation.

Process requirements — Annex I Part II

The vulnerability-handling requirements are unconditional and run for the duration of the product's support period. These obligations are instituted by Article 13.

The product support period

The manufacturer must determine a support period that reflects how long the product is realistically expected to be in use, taking into consideration user expectations, the product's nature/purpose, relevant EU product lifetime laws, comparable products' support periods, availability of the operating environment, support periods of third-party core components, and guidance from the Article 52 administrative cooperation group (ADCO) and the Commission. This must be done proportionately, though Article 13(8) stipulates a **minimum of five years**, unless the product is genuinely expected to be in use for less.

Table 9.
Annex I Part II requirements.

Requirement	Reference
Identify and document vulnerabilities and components, including by drawing up a software bill of materials in a commonly used, machine-readable format, covering at least top-level dependencies.	Annex I Part II(1)
Address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, provide security updates separately from functionality updates.	Annex I Part II(2)
Apply effective and regular tests and reviews of the product's security.	Annex I Part II(3)
Once a security update is available, share and publicly disclose information about fixed vulnerabilities, including a description, an identification of the affected product, the impact, the severity, and the remediation guidance. In duly justified cases, publication may be delayed until users can patch.	Annex I Part II(4)
Establish and enforce a coordinated vulnerability disclosure policy.	Annex I Part II(5)
Facilitate the disclosure of information about potential vulnerabilities in the product and in third-party components, including by providing a contact address for reports.	Annex I Part II(6)
Provide mechanisms to distribute updates securely so that vulnerabilities are fixed or mitigated in a timely manner and, where applicable, automatically.	Annex I Part II(7)
Disseminate security updates without delay and free of charge, with advisory messages telling users what action to take.	Annex I Part II(8)

Article 13(5) adds a due diligence obligation on third-party components, including free and open source components that were never placed on the market. Article 13(6) goes further: after identifying a vulnerability in a component, you must report it upstream to whoever maintains that component, remediate it in your product, and share any code or documentation you produced to fix it.

Raspberry Pi provides robust vulnerability reporting via publications and email. The Raspberry Pi OS build system is designed to make it easy to track and remediate vulnerabilities in the OS and its packages, and to share those fixes back to the community. Further information can be found at https://www.raspberrypi.com/security/.

Support period and retention

Table 10.
Support period and retention obligations.

Requirement	Description	Reference
Support period	Must reflect how long the product is expected to be in use, taking into account reasonable user expectations, the nature and intended purpose of the product, and relevant EU law on product lifetimes. The CRA stipulates **at least five years**, unless the product is expected to be in use for less, in which case the support period matches the expected use time.	Article 13(8)
Justification	The information used to determine the support period must feature in the technical documentation.	Annex VII(4)
Update availability	Each security update issued during the support period must remain available for at least ten years after issue, or for the remainder of the support period — whichever is longer.	Article 13(9)

Requirement	Description	Reference
Disclosure to buyers	The end date of the support period (given, at minimum, as month and year) must be stated clearly at the time of purchase and, where technically feasible, displayed to users on expiry.	Article 13(19)
Documentation retention	Technical documentation and the EU declaration of conformity must be kept available to market surveillance authorities for at least ten years after placement on the market, or for the duration of the support period — whichever is longer.	Article 13(13)
User information	Annex II information and instructions must be kept available to users and authorities on the same ten-year or support-period basis.	Article 13(18)

A five-year support floor with a ten-year update availability tail is a long-lived commitment for an embedded product; it is one of the strongest arguments for choosing a compute platform with a published long-term supply and software support position at the start of a design. Raspberry Pi is committed to backwards compatibility and long-term support for its products, and provides a clear roadmap for the support periods behind its hardware and software. Our longevity data is published on our Product Information Portal.

Product classifications and conformity routes

The CRA establishes product categories that determine the conformity assessment route to be taken. Classification depends on the product's core functionality and deployment context, not on the hardware inside; the same Raspberry Pi Compute Module can power a default-category consumer appliance and an 'Important' Class II firewall. Raspberry Pi Ltd cannot classify your product for you, but we can provide guidance and tools to assist with the implementation of Class I and Class II products.

Table 11.
The CRA product categories and their conformity routes.

Category	Example	Route to conformity	Reference
Default	Anything not listed in Annex III or Annex IV.	Internal production control: Module A via self-assessment.	Article 32(1)(a)
Class I	Annex III Class I — 19 categories including operating systems, boot managers, network management systems, routers, modems, switches, VPNs, password managers, browsers, identity and privileged access management tools, SIEM software, PKI issuance software, physical and virtual network interfaces, microprocessors and microcontrollers with security-related functionalities, security-related ASICs and FPGAs, smart home security products, connected toys with social or location features, and certain wearables.	Module A **only if** harmonised standards, common specifications, or an EU cybersecurity certification scheme at a minimum assurance level of "substantial" (Article 27) are applied in full. Otherwise, Module B plus C, or Module H.	Article 32(2) and Annex VIII
Class II	Annex III Class II — hypervisors and container runtimes, firewalls and intrusion detection or prevention systems, tamper-resistant microprocessors, and tamper-resistant microcontrollers.	Third-party assessment mandatory: Module B plus C, Module H, or an EU cybersecurity certification scheme at a minimum assurance level of "substantial" (Article 27).	Article 32(3) and Annex VIII
Critical	Annex IV — hardware devices with security boxes, smart meter gateways, and other devices for advanced security	An EU cybersecurity certification scheme where required by a delegated	Article 32(4)

Category	Example	Route to conformity	Reference
	purposes, including secure crypto-processors, smart cards, and similar devices featuring secure elements.	act under Article 8(1); otherwise, the same route as Class II.	

Note

Read Article 32.2 carefully.

For a Class I product, Module A's self-assessment is available only when you apply harmonised standards, common specifications, or a recognised certification scheme. Article 32.2 is explicit that where such instruments **do not exist**, the product must go to a notified body under Module B plus C, or Module H. As set out under The current harmonised standards gap, no CRA harmonised standards have yet been cited in the *Official Journal*. Today, a Class I product has no self-assessment route. If your product ships with an operating system as its core functionality, or is a router, modem or switch, this affects you directly.

Two further points on classification. First, Annex III entries are read against the product's **core functionality**: a general-purpose appliance that happens to contain a firewall is not thereby a Class II product, whereas a product whose purpose is to be a firewall is. Recital 45 makes this explicit. Second, Commission Implementing Regulation (EU) 2025/2392 gives the technical description of each Class I, Class II, and critical category. Check your product's core functionality against those descriptions and record your reasoning for any borderline case.

Integrating a component does not by itself change your product's class. Under Article 7(1), building a Class I component, such as an operating system or a boot manager, into your product does not make your product Class I. A general-purpose computer or appliance built on a Raspberry Pi computer is assessed on its own core functionality. You must still assess the security of the whole product, including its components.

Documentation and marking

Table 12.
Documentation and marking obligations.

Deliverable	Content	Reference
Cybersecurity risk assessment	Documented, updated as appropriate during the support period, and included in the technical documentation.	Article 13(2) to (4)
Technical documentation	Eight sections: product description and intended purpose; design, development, production, and vulnerability-handling processes; risk assessment; support period justification; standards applied or solutions adopted in their absence; test reports; a copy of the declaration of conformity; and the SBOM on reasoned request.	Annex VII
User information and instructions	Manufacturer identity and single point of contact; intended purpose; known or foreseeable circumstances that may lead to significant risk; the internet address of the declaration of conformity; support period end date; secure installation, operation, decommission, and update instructions.	Article 13(18), Annex II
EU declaration of conformity	Drawn up on completion of the conformity assessment. Either a full copy or a simplified declaration carrying the exact internet address of the full text must accompany the product.	Article 28, Annexes V and VI
CE marking	Affixed visibly, legibly, and indelibly, alongside the notified body's identification number (where applicable).	Articles 29 and 30

Deliverable	Content	Reference
Single point of contact	Easily identifiable; must let users choose their means of communication, which must not be limited to automated tools.	Article 13(17)
Traceability	Type, batch, or serial number, or another identifying element, included on the product, its packaging, or the accompanying documentation.	Article 13(15)

Reporting obligations from 11 September 2026

Article 14, 'Reporting obligations of manufacturers', sets out two distinct notification paths, which run in parallel via the same Single Reporting Platform (Article 16) to the coordinating CSIRT and ENISA:

- Path 1 — actively exploited vulnerabilities (Article 14(1) to (2))
- Path 2 — severe incidents affecting product security (Article 14(3) to (4))

These follow the same 24-hour/72-hour/final report structure, but they are triggered by different events (exploited vulnerabilities versus severe incidents) and reported separately. Article 14(5) defines what makes an incident "severe" for the purposes of the second path.

Table 13.
Article 14 reporting schedule.

Stage	Actively exploited vulnerability (Article 14(1) and (2))	Severe incident affecting product security (Article 14(3) and (4))
Within 24 hours	Early warning notification indicating, where applicable, the Member States in which you are aware the product has been made available.	Early warning notification stating, at minimum, whether the incident is suspected to be caused by unlawful or malicious acts, and the Member States concerned.
Within 72 hours	Vulnerability notification providing general information about the product, the nature of the exploit and the vulnerability, the corrective or mitigating measures taken, the measures users can take, and how sensitive you consider the information to be.	Incident notification covering the nature of the incident, an initial assessment, the corrective or mitigating measures taken, and the measures users can take.
Final report	**Report issued within 14 days of a corrective or mitigating measure becoming available**; includes a description, an assessment of the severity and impact, information on any malicious actors, and details of the security update or other corrective measure.	**Report issued within one month of submitting the 72-hour notification**; includes a detailed description, an assessment of the severity and impact, the type of threat or likely root cause, and the applied and ongoing mitigation measures.

The 14-day clock starts when a fix or a workaround becomes available, not when the permanent patch ships. A documented mitigation starts the clock.

An incident is severe when it negatively affects, or is capable of negatively affecting, the product's ability to protect the availability, authenticity, integrity, or confidentiality of sensitive or important data or functions; or where it has led or could lead to the introduction or execution of malicious code in the product or in a user's network and information systems (Article 14(5)). A compromise of your own build or update-release channel is the canonical example.

Users must be told, too. Article 14(8) requires you to inform impacted users — and, where appropriate, all users — of the vulnerability or incident and of any mitigation they can deploy (where applicable) in a structured, machine-readable format. If you fail to do so in time, the notified CSIRTs may inform your users themselves.

Only actively exploited vulnerabilities and severe incidents are reportable. A publicly disclosed CVE that is not being exploited in the wild does not start the 24-hour clock; it goes through the ordinary Annex I Part II handling process. The practical difficulty

is that the gap between disclosure and exploitation can be hours, so your triage process must be able to make and record that distinction quickly, escalating it to a named person with authority to file a report if necessary.

Article 15 additionally allows voluntary notification of any vulnerability, cyber threat, incident, or near miss, and Article 14.6 lets the receiving CSIRT request an intermediate status report.

Penalties

Table 14.
Financial penalties.

Infringement	Maximum	Reference
Non-compliance with the Annex I essential requirements, or with the obligations in Articles 13 and 14.	€15,000,000 or 2.5% of total global annual turnover, whichever is higher.	Article 64(2)
Non-compliance with Articles 18–23, 28, 30(1) to (4), 31(1) to (4), 32(1) to (3), 33(5), 39, 41, 47, 49, and 53.	€10,000,000 or 2% of total global annual turnover, whichever is higher.	Article 64(3)
Supplying incorrect, incomplete, or misleading information to notified bodies or market surveillance authorities.	€5,000,000 or 1% of total global annual turnover, whichever is higher.	Article 64(4)

Article 64(5) requires the nature, gravity, and duration of the infringement, any prior fines, and the size and market share of the operator — with express regard to micro, small, and medium-sized enterprises — to be taken into account. Article 64(10) exempts micro and small enterprises from being fined for missing the 24-hour early-warning deadline specifically, and also exempts open source software stewards from being fined altogether. Market surveillance authorities retain their powers to restrict, withdraw, or recall a product (Chapter V) irrespective of any fine.

The current harmonised standards gap

Under Article 27(1), a product that conforms with harmonised standards, or parts of them, whose references have been published in the *Official Journal* of the European Union is presumed to conform to the essential requirements those standards cover. That presumption is the ordinary route to CE marking under the New Legislative Framework, and it is the mechanism that makes self-assessment possible.

As at mid-October 2026, no CRA harmonised standards have been cited in the *Official Journal*. The Article 27 presumption of conformity is therefore unavailable for every product category in every risk class.

Where the work stands

The Commission's standardisation request M/606 was adopted in February 2025 and accepted by CEN, CENELEC, and ETSI on 3 April 2025. It requests around 41 standards, split into horizontal (product-agnostic) and vertical (product-specific) deliverables. Drafting is distributed across several bodies, and the reference number indicates which:

Table 15.
The M/606 deliverable families.

Series	Technical body	Scope
EN 40000	CEN-CLC/JTC 13 WG 9	Horizontal: vocabulary, principles of cyber resilience, vulnerability handling, technical measures. Applies to every product with digital elements.
EN 304 6xx	ETSI (EUSR, within TC CYBER)	Vertical, product-specific categories.
EN 50770	CLC/TC 65X	Operational technology profiles, running alongside the ETSI verticals for equivalent functions.
EN 40001-3 to 40004-3	CEN and CENELEC (CLC/TC 47X for prEN 40001-3)	Semiconductors: microprocessors and microcontrollers with security-related functionalities (prEN 40001-3), tamper-resistant microprocessors and microcontrollers (prEN 40002-3), smart card platforms and secure elements (prEN 40003-3), and security-related ASICs and FPGAs (prEN 40004-3). The first two went to enquiry earlier in 2026 as prEN 50765 and prEN 50766.
EN 18330, EN 40000-10, and EN 40000-11	CEN and CENELEC (CEN/TC 224 for prEN 18330)	Smart card applications (prEN 18330), identity and access management (prEN 40000-10), and hardware devices with security boxes and smart meter gateways (prEN 40000-11).

Progress is real but incomplete. The horizontal EN 40000-1 series has four parts:

Table 16.
Status of the horizontal standards, October 2026.

Standard	Covers	Status
FprEN 40000-1-1	Vocabulary.	Formal vote closed on 1 October 2026 and reported as approved. Publication expected in November 2026.

Standard	Covers	Status
FprEN 40000-1-2	Principles of cyber resilience and product risk management (Annex I Part I(1)).	Same as FprEN 40000-1-1.
prEN 40000-1-3	Vulnerability handling (Annex I Part II).	Comments from the Commission's assessment being resolved before the formal vote. Expected by the end of January 2027.
prEN 40000-1-4	Generic security requirements: threats, security objectives, and controls (Annex I Part I(2)(a) to (m)).	Commission pre-assessment before public enquiry. Expected by 30 October 2027.

ETSI's 18 product-specific standards, EN 304 617 to EN 304 636 and EN 304 642, are further along. All but EN 304 642 have passed public enquiry. ETSI EN 304 623 (boot managers) has a planned timeline: final vote from December 2026, publication in January 2027, and citation in the *Official Journal* in April 2027. Public drafts are available from ETSI at https://docbox.etsi.org/CYBER/EUSR/Open.

Two caveats matter more than the drafting progress:

- First, **ratification as an EN is not the same as citation in the *Official Journal***. Adoption by CEN, CENELEC, or ETSI is a necessary step, not a sufficient one. The Commission must assess the standard against the mandate and cite its reference in the *Official Journal* before Article 27 applies. That assessment takes time, and the CRA gives no deadline for it.
- Second, not every standard will be cited. The amendments to EN IEC 62443-4-1 and 62443-4-2 will not be cited in the *Official Journal*, although the industrial vertical standards (the EN 50770 series) are derived from them. Product-specific standards are expected to be cited: EN 304 623 is planned for April 2027. Check each standard you rely on for its citation status, not just its publication.

Note

Confidence note. The status information in this section comes from the CEN-CENELEC and ETSI status matrices dated 30 September 2026, and from later public reports. It is not drawn from an *Official Journal* citation or a formal CEN-CENELEC decision. It provides the best available picture at the date of this release, and should be re-checked before being relied upon in any compliance plan. Only publication in the *Official Journal* is determinative.

How this impacts the assessment of products by their product class

Table 17.
Practical effect of the standards gap.

Class	Consequence today
Class I	Article 32(2) removes Module A where harmonised standards do not exist. A notified body under Module B plus C, or Module H, is required. Chapter IV has only applied since 11 June 2026, so the notified body population is new and its capacity untested.
Class II and Critical	Third-party assessment or certification was always required, so the standards gap alters this route less. It does, however, change the technical benchmark the notified body will assess you against, which is not yet fixed.

Planning without a presumption of conformity

The absence of harmonised standards is not a reason to wait. Article 27 is a convenience, not a precondition: Annex VII(5) expressly contemplates the case where harmonised standards have not been applied, and requires "descriptions of the solutions adopted to meet the essential cybersecurity requirements" instead. A rigorous, traceable decision trail is a complete alternative route — it takes more work to build and more work to defend.

There are four things you can do now that will not be wasted whichever way citation lands:

1. **Build the decision trail, requirement by requirement.** For each of the 13 requirements under Annex I Part I point 2, record the risk assessment finding that makes it applicable or not, the design decision taken, and the test evidence. Structure it so that a standard reference can be slotted in later against each row. The draft prEN 40000-1-4 links each essential requirement to threats, then to security objectives, then to the controls an assessor will test. Following the same chain now will make mapping straightforward later on.
2. **Adopt the existing standards as technical benchmarks.** None of them carry a CRA presumption of conformity, and you should say so explicitly in your documentation, but they encode the right engineering and are what the eventual harmonised standards will largely be built from (see the table below).

Table 18.
Interim indicative standards.

Standard	Scope
ETSI EN 303 645	The IoT cybersecurity baseline: secure defaults, no universal default passwords, vulnerability disclosures, update mechanisms, and attack-surface minimisation. Maps closely onto Annex I. Raspberry Pi Ltd's fourth- and fifth-generation compute platforms were among the first to be fully compliant.
EN 18031-1/-2/-3	Harmonised under the Radio Equipment Directive in 2025 for Article 3(3)(d), (e), and (f). Directly relevant when your product is radio equipment, and a useful proxy elsewhere.
IEC 62443 series	Industrial automation and control systems. IEC 62443-4-1 (secure development lifecycle) and 4-2 (component requirements) form the expected technical basis for the OT verticals. The risk-analysis approach in 62443-4-1 is being used across the EN 50770 series.
Draft EN 40000-1 series and ETSI EN 304 6xx	The drafts of the CRA standards themselves (see Table 16). Use them to check the shape of your evidence, but do not cite their clause numbers until the final texts are published.
ISO/IEC 15408 (Common Criteria)	Where a target Evaluation Assurance Level applies, or where an EUCC certificate may later provide a presumption route under Article 27(8).

Use mature standards now rather than waiting for the drafts. Keep your mappings under version control, do not rely on draft clause numbers, and update the mappings when the *Official Journal* citations arrive.

3. **Plan the Important Class I route on the assumption you will need third-party assessment.** Notified body engagement has a lead time, and if citation arrives late, a queue will form quickly. Budget and schedule for Module B plus C, or Module H, and treat a later switch to Module A as an upside.
4. **Watch for common specifications.** Where standardisation is blocked or delayed, Article 27(2) to (5) empowers the Commission to adopt common specifications by an implementing act as a fallback, which would carry the same presumption. None have been adopted to date. If the 2026 mandate deadlines slip materially, this becomes the mechanism to watch.

Note finally that the Commission's Article 26 guidance, approved on 27 July 2026 (C(2026) 5252), is the most substantial interpretive material available. It is expressly non-binding and changes no obligation or date, but it is the Commission's own answer to the questions manufacturers ask most. It is aimed particularly at small and medium-sized enterprises (SMEs).

Conducting the cybersecurity risk assessment

The risk assessment is the load-bearing document. Article 13(2) requires you to undertake one and to consider its outcome during planning, design, development, production, delivery, and maintenance. Article 13(3) states what it must contain. Article 13(4) places it in the technical documentation. Annex VII(3) makes it an explicit heading there. And Annex I Part I point 2 applies only "on the basis of" it. Everything else is downstream.

The CRA risk assessment requirements

Table 19.
CRA risk assessment.

Requirement	Detail	Reference
Documented	Must be written down and updated as appropriate during the support period.	Article 13(3)
Scoped to real use	Must analyse cybersecurity risks based on the **intended purpose and reasonably foreseeable use** of the product, along with the **conditions of its use**; for example, the operational environment and the assets to be protected.	Article 13(3)
Time-bounded	Must take into account the length of time the product is expected to be in use.	Article 13(3)
Requirement-mapped	Must indicate **whether and in what manner** each Part I point 2 requirement applies and how it is implemented, as informed by the assessment.	Article 13(3)
Process-mapped	Must indicate how you apply Part I point 1 and the Part II vulnerability-handling requirements.	Article 13(3)
Justified in its exclusions	Where an essential requirement is not applicable, a clear justification must be included in the technical documentation.	Article 13(4)
Maintained	Cybersecurity aspects, including vulnerabilities you become aware of and relevant third-party information, must be systematically documented, with the risk assessment updated where applicable.	Article 13(7)

The CRA prescribes no methodology — you may use any defensible one. The following uses **NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments***, because it is public, free, widely recognised, and structured in a way that maps nicely to the requirements of Article 13(3). IEC 62443-3-2 and ISO/IEC 27005 are equally legitimate choices.

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* will be referred to as **SP 800-30r1** going forwards.

Structuring the assessment: SP 800-30r1 mapped to the CRA

SP 800-30r1 sets out a four-step process. Below is a table that maps each step to the CRA.

Table 20.
SP 800-30r1 process mapped to CRA obligations.

SP 800-30r1 step or task	Scope	Corresponding CRA article
Step 1: Prepare	Purpose, scope, assumptions and constraints, information sources, and the risk model and analytical approach. For a CRA assessment, this is where you fix intended purpose, reasonably foreseeable use, operational environment, assets to be protected, and	Article 13(3)

SP 800-30r1 step or task	Scope	Corresponding CRA article
	expected in-use lifetime. Get this wrong and every later finding is out of scope.	
Step 2, task 1: Identify threat sources and threat events	A threat-source inventory with, for adversarial sources, assessed capability, intent, and targeting; along with a set of threat events, ideally assembled into threat scenarios rather than isolated events. Appendices D and E give exemplary taxonomies.	Annex VII(3)
Step 2, task 2: Identify vulnerabilities and predisposing conditions	Weaknesses in the product, as well as conditions of deployment that raise or lower the chance that an initiated threat event causes harm. Your SBOM plus a scanner output is an input here, not the answer: architectural and configuration weaknesses will not appear in a CVE feed. See Appendix F.	Annex I Part I(2)(a) and Part II(1)
Step 2, task 3: Determine likelihood	Likelihood of initiation or occurrence, likelihood that initiation results in adverse impact, and the combination of the two. See Appendix G.	Article 13(3) (as quantum of risk)
Step 2, task 4: Determine impact	Magnitude of harm from loss of confidentiality, integrity, or availability. Article 13(2) of the CRA explicitly extends this to the health and safety of users, which most IT-oriented impact scales omit — include it. See Appendix H.	Article 13(2)
Step 2, task 5: Determine risk	Risk as a function of likelihood and impact per threat event or scenario. See Appendix I. **This is the output Article 13(3) consumes:** it determines which Annex I Part I point 2 requirements apply and how.	Article 13(3)
Step 3: Communicate results	The written assessment. Appendix K lists the elements of a risk assessment report. This maps to Annex VII(3) and drives the "circumstances which may lead to significant cybersecurity risk" that Annex II requires you to tell users about.	Annex VII(3) and Annex II
Step 4: Maintain	Monitor risk factors and update accordingly. Article 13(3) and (7) make this obligatory for the whole support period, so build the trigger conditions in: new CVE in a shipped component, new deployment environment, feature update, incident.	Article 13(3) and (7)

Choose and declare your scales

SP 800-30r1 supports qualitative, quantitative, and semi-quantitative assessment. For most embedded products, a semi-quantitative approach gives the best balance: numeric bins support relative prioritisation, while the qualitative labels communicate to reviewers and notified bodies. Whichever you pick, define the scales once in the document and use them consistently — the repeatability of the assessment is important. The values provided here are illustrative; you should define your own and document the reason for setting those values in the risk assessment.

Table 21.
Illustrative risk matrix scale, aligned to the SP 800-30r1 scale used across Appendices D to I.

Qualitative	Semi-quantitative range	Representative value	Example likelihood reading
Very High	96–100	10	Almost certain, or occurring more than 100 times a year
High	80–95	8	Highly likely, or occurring tens of times a year
Moderate	21–79	5	Somewhat likely, or occurring several times a year
Low	5–20	2	Unlikely, but possible within the assessment window
Very Low	0–4	0	Highly unlikely

You should also declare your **analysis approach**. SP 800-30r1 distinguishes three starting points: threat-oriented (start from threat sources and events), asset/impact-oriented (start from the consequences and assets you care about), and vulnerability-oriented (start from known weaknesses). Each reaches the same risk factors in a different order, and each biases what gets found.

A short worked example

The following is one row of a risk register for a hypothetical industrial gateway built on a Raspberry Pi Compute Module 5 running a custom Linux image, deployed on customer plant networks and reachable from a corporate LAN. It is deliberately compressed; a real register would run to dozens of rows, and each would carry its own rationale for the assessed values.

Table 22.
CRA risk assessment example.

Field	Entry
Asset and consequence of concern	Integrity of control commands issued to downstream PLCs; availability of the gateway's essential function.
Threat source	Adversarial, external, financially motivated. Capability: High. Intent: High. Targeting: Moderate — opportunistic scanning of exposed management interfaces rather than a targeted attack on this OEM.
Threat event	Adversary reaches an exposed network management service, authenticates using a credential shared across the fleet, and issues arbitrary commands.
Vulnerabilities	Management service enabled by default; password authentication permitted; a single factory-set credential common to all units; no rate limiting on authentication attempts.
Predisposing conditions	Device routinely deployed on a flat network with no segmentation from the corporate LAN. Customers rarely change factory credentials.
Likelihood of initiation	High — internet-wide scanning for this service class is continuous.
Likelihood of adverse impact	High — no compensating control between authentication and command execution.
Overall likelihood	High.
Impact	Very High — loss of control integrity in a plant environment endangers the health and safety of users, which Article 13(2) requires to be considered.
Level of risk	Very High.
Annex I requirements engaged	(b) secure by default; (d) protection from unauthorised access and reporting of possible unauthorised access; (j) limit attack surfaces; (h) availability and anti-DoS; (l) recording and monitoring of relevant internal activity.
Risk response	Management service disabled by default and bound to a dedicated interface; per-device credentials provisioned at manufacture; public-key authentication allowed only; authentication rate limited; authentication events logged and exportable. Deployment guidance in the Annex II user information requires network segmentation.

Field	Entry
Residual risk and owner	Moderate — named engineering owner; re-assessed on any change to the exposed interface set.
Evidence	Interface inventory, provisioning records, penetration test report reference, configuration baseline hash.

This fragment illustrates three things:

- The predisposing condition — flat customer networks — is not a defect in the product, but it materially changes likelihood and is exactly the kind of “condition of use” Article 13(3) requires you to analyse.
- The impact assessment considers health and safety, not just data security.
- The response links back to specific lettered requirements in Annex I, which is what makes the assessment usable as Annex VII(3) evidence rather than a standalone security exercise.

Documenting non-applicability

A common failure is to leave inapplicable requirements blank. Article 13(4) requires a clear justification. A defensible entry names the requirement, states why it does not apply given the intended purpose, and — where you have nonetheless identified risk in that area — says what you did instead. See the example below.

Note

Annex I Part I(2)(m), secure permanent removal of data and settings. The product processes no user-supplied or personal data; all configuration is provisioned at manufacture and is not user-modifiable. No user-accessible data or settings exist to remove, so the requirement is not applicable. Residual risk from recovery of the provisioned configuration is addressed under (e) by full-disk encryption, with a device-unique key bound to the hardware, and the Annex II decommissioning instructions direct the user to destroy the storage device.

Turning an SBOM into a vulnerability list

Annex I Part II(1) requires an SBOM to be provided in a commonly used, machine-readable format. Raspberry Pi OS generates a full SBOM for every release using the open source tool `syft`, and `rpi-image-gen` includes native SBOM generation in both SPDX and CycloneDX. To convert this into a vulnerability list, `grype` scans the SBOM against current CVE databases:

Code

```
grype sbom:/path/to/sbom.json
```

`grype` refreshes its vulnerability database before each scan, so the result is a point-in-time snapshot. A scan that returns nothing today may return several items tomorrow. A single scan during manufacture does not satisfy Annex I Part II(2) or (3): run scans on a schedule, re-scan after significant upstream security announcements, and keep a triage record showing how each finding was assessed against your deployed software state.

Note the difference between deployment models here. A fixed, non-updatable product has a static SBOM captured at manufacture — this is simpler to produce, but offers no remediation path if a CVE appears later. An updatable product’s SBOM must reflect the software state actually deployed, which requires you to track SBOM state across the fleet.

Why choose Raspberry Pi?

Raspberry Pi Ltd provides robust compliance tools and support across the platform layer of your applications. This section maps the available tools to the specific regulatory obligations they help fulfil.

Table 23.

Raspberry Pi tooling mapped to CRA obligations.

Raspberry Pi tool	Functional summary	Requirements it supports
`rpi-image-gen`	Tool for building custom Linux images for your own product. Native SBOM generation in SPDX and CycloneDX, and A/B image support for atomic updates with automatic rollback. Produces image description provisioning (IDP) artefacts carrying partition, encryption, and storage metadata.	Annex I Part II(1), SBOM; Part I(2)(b), secure defaults; Part I(2)(c) and Part II(7), secure, recoverable update mechanism; Part I(2)(j), attack surface
`pi-gen`	The current distribution-build tooling, used to build Raspberry Pi OS itself. Uses pre-built upstream Debian packages without alteration, which makes vulnerability tracking against Debian advisories straightforward — an advantage over build systems that patch or rebuild packages.	Annex I Part II(1) and (2); traceable software provenance for Annex VII(2)
`pi-gen-micro`	Device image builder with a strong emphasis on reduced functionality and a smaller attack surface. Intended for full-system-update deployment models or bespoke provisioning functionality.	Annex I Part I(2)(j), attack surface; Part I(2)(k), impact reduction
`rpi-sb-provisioner`	Secure Boot Provisioner. Converts a prepared OS image into a signed secure-boot image and automates factory provisioning: signing-key programming, full-disk encryption with device-unique keys bound to the hardware, and image deployment. Three modes: `secure-boot`, `fde-only`, and `naked`. Supports Raspberry Pi 5, Raspberry Pi 4 Model B, Raspberry Pi Compute Module 5, Raspberry Pi Compute Module 4, and Raspberry Pi Zero 2 W. Maintains a manufacturing database of serial numbers, MAC addresses, provisioning timestamps, and security configurations. Supports PEM and PKCS11 signing keys, so the signing key can live in an HSM.	Annex I Part I(2)(d), unauthorised access; Part I(2)(e), confidentiality of data at rest; Part I(2)(f), integrity of programs and configuration; Part I(2)(c), authenticated update path; and Article 13(15), product identification and traceability
Raspberry Pi Connect	Secure remote access to a deployed Raspberry Pi from a browser, with remote-update functionality for devices already in the field.	Annex I Part II(7) and (8), secure, timely update distribution
`syft` / `grype`	Open source SBOM generation and CVE scanning. Raspberry Pi OS publishes a `syft`-generated SBOM for every release,	Annex I Part II(1), (2), and (3)

Raspberry Pi tool	Functional summary	Requirements it supports
	which can serve as a reference for OEM builds.	
Raspberry Pi security advisories	Advisories for software written or modified by Raspberry Pi Ltd — kernel, firmware, bootloader, VideoCore GPU drivers, and Raspberry Pi–specific tools.	Annex I Part II(4) and (6); Article 13(6), component vulnerability handling
Vulnerability disclosure policy	A published coordinated vulnerability disclosure procedure and contact address for Raspberry Pi products.	Annex I Part II(5) and (6), as an upstream input to your own policy
Product Information Portal	A repository for application notes and white papers on implementing security measures, maintained by an internal CRA working group that tracks the regulation and the standardisation work.	Annex VII, technical documentation

Secure boot and the draft boot manager standard

Boot managers are in the Class I category, and ETSI EN 304 623 is being prepared as their harmonised standard. If secure boot matters to your risk assessment, two features of the draft are worth knowing:

- The draft describes an 'open device' use case, where the chip maker leaves boot configuration and keys to the manufacturer of the end product. This is how Raspberry Pi secure boot works: it is off when the product ships, and you program your own key and choose your own boot configuration at manufacture using `rpi-sb-provisioner`.
- The draft forbids global secret keys for symmetric verified boot. Raspberry Pi verified boot uses public-key signatures, so no secret key is shared across devices. Your private signing key stays with you and can be held in a hardware security module.

The standard is still in draft. Check the final text when it is published, which is expected in January 2027.

Raspberry Pi OS and your monitoring

Raspberry Pi Ltd directly maintains a small set of packages: the kernel, the firmware, the bootloader, the VideoCore GPU drivers, and a handful of Raspberry Pi–specific tools. The overwhelming majority of software in a Raspberry Pi OS–based product comes from upstream Debian, where the Debian Security Team manages CVE tracking and patches.

Monitoring both sets is your obligation under Annex I Part II(1) to (3). In practice, that means three subscriptions and one process:

- Raspberry Pi Ltd security advisories for the platform packages.
- `debian-security-announce` for the Debian package set.
- Advisories for any component you added yourself, including vendored open source libraries that appear in your SBOM but in neither of the above.
- A documented triage process that assesses each incoming advisory against your deployed software inventory and records the outcome — including "not applicable", and why.

Raspberry Pi Ltd relies on the stewardship of upstream Debian for vulnerability reporting and fix distribution. Using our platform allows integrators to leverage that stewardship, rather than having to build their own vulnerability monitoring and patching infrastructure from scratch.

The Raspberry Pi support model

Raspberry Pi Ltd offers a set of tools and services to help you easily meet your CRA obligations. This is in keeping with our flexible, open source, and general-purpose computing model. Here is a summary of the capabilities Raspberry Pi Ltd provides and the responsibilities of the integrator:

Table 24.
Division of responsibility.

Raspberry Pi Ltd does	Raspberry Pi Ltd does not
Build a general-purpose image with known, documented content	Classify your product under Annex III or IV, or choose your conformity assessment route
Generate an SBOM for software content in a standard format	Write or own your cybersecurity risk assessment
Provide signed and secure boot, and full-disk encryption with device-unique keys	Carry out vulnerability monitoring for non–Raspberry Pi software in your product
Field update facilities via `apt`, A/B booting, and Raspberry Pi Connect	Post-sale monitoring of your fleet, or communication with your users
Report vulnerabilities and publish advisories for Raspberry Pi software	File your Article 14 notifications, or determine your support period
Prepare documentation and guidance to feed your technical file	Assess whether that documentation meets the needs of your technical file

Raspberry Pi Ltd will not act as your notified body, and its own conformity does not transfer to your product — conformity assessment and placement of the product on the market remain your obligations to complete.

Raspberry Pi Connect

Four CRA requirements combine into a single operational problem:

- Annex I Part II(2) requires you to remediate vulnerabilities **without delay**.
- Annex I Part II(7) requires **mechanisms to distribute updates securely** so that vulnerabilities are fixed or mitigated in a timely manner.
- Annex I Part II(8) requires that available updates are disseminated **without delay and free of charge**.
- Article 14(2)(c) gives you fourteen days from a corrective or mitigating measure becoming **available** to file a final report describing the update you have **made to remedy the vulnerability**.

Now, consider where your product actually lives. It sits on a customer's plant network behind a firewall you do not administer, with no inbound reachability — possibly powered down for a fortnight and owned by someone who has never logged in to it. You have a patch. The regulation assumes you can deliver it.

But that delivery path is the hard part, and it is not a coding problem. It is infrastructure — you need a device identity system, an authenticated egress channel, an artefact integrity mechanism, a deployment record, and a way to know what software version each unit is actually running. Building that yourself is a multi-quarter project; Raspberry Pi Connect is a simple `apt install` away.

What is Raspberry Pi Connect?

Raspberry Pi Connect provides secure access to your Raspberry Pi from anywhere through a browser. It is installed by default in Raspberry Pi OS Desktop and Full; a **Lite** variant supporting remote shell only, with no screen-sharing capability, is installed by default in Raspberry Pi OS Lite. It requires Raspberry Pi OS **Bookworm** or later.

Three capabilities are exposed per device, each independently controllable: **screen sharing**, **remote shell**, and **remote update**. For an OEM product, the remote update capability is the one that matters, while the first is usually irrelevant, making headless Lite builds that cannot screen share the optimal default.

Communication is encrypted and, by default, direct between the device and the browser. Where a direct connection cannot be established, a relay server is used, in which case Raspberry Pi retains only the metadata required to operate the service. All connections are **outbound** from the device: the Raspberry Pi initiates, so there is no inbound listener to expose and no port to open on the customer's firewall.

Note

The architectural advantage: An outbound-only update channel is not merely convenient. It allows you to satisfy Annex I Part II(7) — which asks for secure, timely update distribution — **without** adding a network-facing service to the product. Adding such a service would directly conflict with the obligation to minimise attack surfaces, including external interfaces, under Annex I Part I(2)(j). While most bespoke remote-management designs trade one requirement for the other, Raspberry Pi Connect satisfies both.

Access is managed through Raspberry Pi ID, with two-factor authentication available. Devices are linked using **auth keys**: single-use, time-limited tokens, one per device, that can be baked in during imaging through Raspberry Pi Imager or passed to `rpi-image-gen` at build. Connect signs communication with the device's serial number, so moving storage media between units breaks the link rather than silently cloning an identity.

Two update mechanisms

Raspberry Pi Connect supports two update options. Choosing between them is an important CRA and engineering decision.

Table 25.
A/B boot updates versus script artefacts.

	A/B boot updates	Scripted updates
Built with	`rpi-image-gen`	`otamaker`, from the `rpi-connect-ota` package

	A/B boot updates	Scripted updates
What it does	Replaces the entire operating system. Two independent slots, each with its own boot and system partition. The device boots the new slot and **automatically reverts to the known working slot if that fails**.	Runs a shell script as root on the device. Exit code reports the outcome: success, failure, or success-plus-reboot-required.
Prerequisites	Raspberry Pi 4 Model B or later devices must be imaged once into an A/B layout; this requires physical access and at least 16GB of storage. Raspberry Pi 5 and later devices that use EEPROM boot can also be configured to use A/B boot updates.	None beyond Connect and the `rpi-connect-ota` package. Works on a standard Raspberry Pi OS installation with any partition layout.
Recovery on failure	**Automatic rollback.**	**None.** Test carefully before deploying remotely.
Best CRA fit	The primary update path for a product with a five-year-plus support period. Directly supports Annex I Part I(2)(c) and, critically, Part I(2)(h) — availability of essential and basic functions, even after an incident.	Fast remediation and maintenance where an A/B layout is not in place: package upgrades, configuration changes, and mitigations pending a full image.

The rollback property is worth considering when updating devices in the field. This document's guidance on fixed versus updatable products notes that a failed update must not leave a device unrecoverable. A/B boot is that guarantee.

Deployment is the same for both: build the artefact, host it anywhere the recipient device can reach it. The location does not need to be reachable from Raspberry Pi's servers or from the public internet. Raspberry Pi Connect can be used to provide a secure pipeline to deliver the update, and that pipeline is entirely under the control of the integrator.

Mapping Raspberry Pi Connect capabilities to CRA requirements

Table 26.
Raspberry Pi Connect capabilities mapped to CRA obligations.

Connect capability	CRA or engineering requirement	Reference
Outbound-only encrypted channel; no inbound listener on the product.	Secure update distribution without adding an external interface or requiring a customer firewall change.	Annex I Part II(7) and I(2)(j)
Updates are deliverable to devices behind a firewall, and also to offline devices, which are updated the next time they sign in.	Dissemination "without delay" measured against a real installed base, not an idealised one. Removes the excuse that the fleet was unreachable.	Annex I Part II(2) and II(8)
A/B boot update with automatic revert to the last known working slot.	Updates can be applied without risk of rendering the device unrecoverable; availability of essential functions is preserved after a failed update.	Annex I Part I(2)(c) and I(2)(h)
SHA-256 checksum registered per artefact and verified by the device before application.	Integrity of programs and configurations against unauthorised modification — independent of the transport used to fetch the payload.	Annex I Part I(2)(f) and II(7)
Deployment records cannot be deleted once deployed or attempted, providing traceability if an account is compromised.	Tamper-evident record of **what** was shipped, **when**, and **to which devices** — the exact content the final report and technical documentation from Article 14 require.	Article 14(2)(c)(iii) and 13(7) — this may also be used to justify compliance during a product's design, and to supply evidence in support of Annex VII(2)(b)

Connect capability	CRA or engineering requirement	Reference
		and VII(6) in the technical construction file
`cat /etc/rpi-issue` returns the `rpi-image-gen` commit and the deployed artefact version.	Per-device attestation of the software state actually running, so your SBOM reflects the deployed fleet rather than the build server.	Annex I Part II(1)
Per-device single-use auth keys, provisioned during imaging. Communication signed with the device serial number.	Device identification and traceability. Protection against unauthorised access through per-unit, rather than shared, credentials.	Article 13(15) and Annex I Part I(2)(d)
Runs as a user-level service, not as root. Screen sharing, remote shell, and remote update are each independently opt-in (`rpi-connect vnc off`, `shell off`, `ota on`). Lite has no screen-sharing capability.	Secure-by-default configuration and minimised attack surface: an OEM product can ship with update capability enabled and interactive access disabled.	Annex I Part I(2)(b) and Annex I Part I(2)(j)
Script output recorded in the `systemd` journal (`journalctl -t rpi-ota-connector`); deployment status reported as Pending, In Progress, Succeeded, or Failed.	Verifiable evidence per device that remediation actually landed — the difference between "we published a patch" and "the fleet is patched".	Annex I Part II(2) and Article 13(7)
Connect for Organisations: multiple users, device tags, search and filter, an audit log, bulk provisioning, and a management API.	Operationalises Part II at fleet scale, and gives you the access record a market surveillance authority or notified body will ask about.	Annex I Part II(2) to (8) and Article 13(7)

Article 14 and the fourteen-day reporting window as a worked example

Article 14 places requirements upon the manufacturer to ensure timely reporting and appropriate mitigation of security vulnerabilities. The illustration below shows how this is possible using the tools Raspberry Pi Ltd provides for both upstream reporting and downstream deployment. Elapsed times are illustrative only.

Table 27.
Article 14 reporting supported by a Raspberry Pi Connect update channel.

Elapsed time	Action	Reference
T+0	A scheduled `grype` scan against your SBOM flags a CVE in a shipped component. Internal threat assessment establishes an active exploitation.	Annex I Part II(3)
< 24h	File an early warning on the ENISA Single Reporting Platform, naming the affected product and the Member States in which you know it has been made available. In parallel, tag the affected device group in Raspberry Pi Connect, using your existing inventory.	Article 14(2)(a)
< 72h	Issue a vulnerability notification stating the nature of the exploit and the mitigation users can apply. If a configuration change is enough for now, a **script artefact** will deploy it to the fleet today, allowing you to report a mitigating measure rather than just a notification.	Article 14(2)(b)

Elapsed time	Action	Reference
Days 2–5	Build the fixed image with `rpi-image-gen`, host the `.tar.zst` artefact, register its URI and SHA-256, and deploy it to the tagged group. Devices behind customer firewalls pull it; devices that are powered off collect it on next sign-in. Where appropriate, inform impacted users of the vulnerability and the remediation in a structured, machine-readable format. Do not wait for the final report.	Annex I Part II(2) and (7) Article 14(8)
Days 5–14	Confirm uptake. Deployment status per device, plus `/etc/rpi-issue` artefact versions, tell you what proportion of the fleet is remediated and which units are outstanding.	Annex I Part II(2)
≤ 14 days	Final report is filed, including “details about the security update or other corrective measures that have been made available”. The undeletable deployment record **is** that evidence.	Article 14(2)(c)

Without a delivery mechanism, steps four to seven are aspirational. You can file the paperwork, but the final report will describe an update nobody received, and you will remain exposed under Annex I Part II(2) and (8) for as long as the fleet stays unpatched.

In summary: the operational case for Raspberry Pi Connect

The CRA’s vulnerability-handling obligations run for at least five years and are judged on outcomes in the field, not intentions in the repository. Authenticated device identity, artefact integrity verification, automatic rollback, per-device version attestation, and an immutable deployment record are precisely the infrastructure those obligations assume you have built — with Raspberry Pi Connect, that work has been done for you. By choosing an A/B layout during the design stage and opting each device in to remote updates during provisioning, the hardest operational aspect of CRA compliance becomes an active deployment you can point a notified body at.

What to do now

The reporting obligation has applied since 11 September 2026, and it covers every in-scope product already on the market. If your reporting process is not yet in place, start with the first six actions below. The rest lay the foundation for full application on 11 December 2027.

Table 28.
CRA action checklist.

Action	Drives
List every product in scope, including products you no longer sell or support. Reporting applies to all of them.	Articles 14 and 69(3)
Establish the software inventory. Generate an SBOM for every shipped software configuration, not just the current one. Debian package management and `syft` give you a starting point; `rpi-image-gen` produces SPDX or CycloneDX for custom builds.	Annex I Part II(1)
Subscribe and triage: Raspberry Pi Ltd advisories, `debian-security-announce`, and advisories for any components you added. Write down the triage process, including how a disclosed vulnerability is distinguished from one under active exploitation.	Annex I Part II(2) and (3)
Publish a coordinated vulnerability disclosure policy and a contact address, and make sure a human reads it.	Annex I Part II(5) and (6)
Delegate the incident response process. Name the person with authority to file on the Single Reporting Platform, identify the CSIRT serving as coordinator for your Member State of main establishment, and practise producing a defensible 24-hour early warning based on partial information. Build the process into your quality management system and test it end to end.	Article 14
Prepare the user-notification channel. Article 14(8) requires you to inform impacted users, where appropriate, in a structured, machine-readable format. Decide the mechanism before you need to use it.	Article 14(8)
Agree a ship-hold process so that you can stop shipments quickly when a serious vulnerability is found in a product you are still selling.	Annex I Part I(2)(a) and Part II(2)
Classify the product and decide the conformity route, recording your reasoning. If it is Important Class I, start the notified body conversation now.	Articles 7, 8, and 32
Determine and justify the support period, presenting the end date to buyers at point of sale.	Articles 13(8) and (19)
Start the risk assessment. Since it gates which Annex I requirements apply, nothing else in the technical file can be finished without it.	Article 13(2) to (4)
Settle the update architecture. If the answer is currently “no field updates”, revisit it now rather than in 2027.	Annex I Part I(2)(c) and Part II(7)
Ask your suppliers whether they will still supply your components after 11 December 2027. Some suppliers may withdraw products rather than ensure they are compliant. Raspberry Pi Ltd will continue to supply its products after that date.	Article 13(5) and (8)
Prepare your website for the information the CRA requires you to publish, such as the support period end date, the declaration of conformity, user instructions, and security advisories and updates.	Article 13(18) and (19), Annex II

Note

Reporting platform: ENISA’s Single Reporting Platform, the entry point for all Article 14 notifications, has been live since 11 September 2026 at https://portal.cra-srp.enisa.europa.eu. Register before you need it. Voluntary notifications under Article 15 and an API for automated reporting are not yet available. Build your internal process so that it produces the required content in time, and treat the filing itself as the last step.

References

Legislation and official sources

- Regulation (EU) 2024/2847 (Cyber Resilience Act), OJ L, 2024/2847 (20 November 2024)
- European Commission, Cyber Resilience Act implementation — Frequently asked questions (first published 3 December 2025, updated periodically)
- European Commission, Article 26 guidance on applying the Cyber Resilience Act, C(2026) 5252 (approved 27 July 2026)
- European Commission, Cyber Resilience Act — reporting obligations
- Commission Implementing Regulation (EU) 2025/2392 on the technical description of the categories of important and critical products with digital elements (OJ L, 1 December 2025)
- Regulation (EC) No 765/2008; Decision No 768/2008/EC (conformity assessment modules A, B, C and H)
- Regulation (EU) 2019/1020 (market surveillance), as amended by CRA Article 66
- ETSI EN 303 645 V3.1.3 — IoT cybersecurity baseline standard
- ENISA CRA requirements and standards mapping

Standards and methodology

- Standardisation request M/606 (accepted by CEN, CENELEC, and ETSI on 3 April 2025)
- ETSI EN 303 645, Cyber security for consumer Internet of Things: baseline requirements
- EN 18031-1, −2 and −3, harmonised under Directive 2014/53/EU (RED) Article 3(3)(d), (e) and (f)
- IEC 62443 series, in particular IEC 62443-4-1 and IEC 62443-4-2
- ISO/IEC 15408 (Common Criteria); Commission Implementing Regulation (EU) 2024/482 (EUCC)
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments (September 2012)
- NIST SP 800-39, Managing Information Security Risk, for the three-tier risk management hierarchy

Raspberry Pi and open source tooling

- `rpi-sb-provisioner`
- `rpi-image-gen`
- `pi-gen`
- `pi-gen-micro`
- `raspi-config`
- `syft`
- `grype`
- Debian security advisories
- Raspberry Pi security advisories and coordinated vulnerability disclosure policy
- Raspberry Pi Connect
- Raspberry Pi Product Information Portal

Related regimes

- UK Product Security and Telecommunications Infrastructure Act 2023 and the Product Security (Security Requirements for Relevant Connectable Products) Regulations 2023. Compliance with ETSI EN 303 645 satisfies the security requirements of the 2023 Regulations, though the UK and EU regimes are not directly equivalent.
- Directive 2014/53/EU (RED) Article 3(3)(d), (e) and (f), and Commission Delegated Regulation (EU) 2022/30. RED cybersecurity compliance is relevant to, but not a substitute for, CRA compliance.
- Directive (EU) 2022/2555 (NIS 2) and Directive (EU) 2024/2853 (product liability). Both interact with CRA obligations.

Contact us for more information

Please contact applications@raspberrypi.com if you have any queries about this white paper.

Web: www.raspberrypi.com

Raspberry Pi

Raspberry Pi is a trademark of Raspberry Pi Ltd

Raspberry Pi Ltd