TITLE	Owasys Cyber Resilience Act (CRA) Compliance Path and Shared Responsibility Model	Author(s) Mikel Fernández	Date 2026/10/19
Abstract	A Guide for Integrators and Solution Developers on the Owasys Platforms	Approved Miguel López	Project Owasys

PUBLIC

This document may be shared freely with integrators, customers, and external auditors as part of CRA compliance assistance.
© OWASYS S.L. (OWASYS Advanced Wireless Devices™).

TABLE OF CONTENTS

1 Target Level of CRA Compliance for Owasys Platforms....3
1.1 CRA Classification....4
2 Documentation and Compliance Artifacts Provided by Owasys....5
3 The Owasys Shared Responsibility Model (SRM)....7
3.1 Owasys Responsibilities (Platform Security):....7
3.2 Customer/Integrator Responsibilities (Application Security):....7
3.3 Updates on Debian-based firmware....8
3.4 Customer reporting to Owasys....9
4 Owasys CRA Compliance Roadmap....10

DOCUMENT HISTORY

Rev.	Date	Author(s)	Description
P1A	03/17/2026	Mikel Fernández	First draft
A	03/18/2026	Mikel Fernández	Add references and corrected minor typos.
B	05/15/2026	Mikel Fernández	Add customer reporting and 3rd-party interfaces
C	10/05/2026	Mikel Fernández	Revised after D26-0006/D25-0015 policy changes
PD1	2026/10/07	Mikel Fernández	Alignment with Security Centre; Art 14 severe incidents and final-report deadlines
PD2	2026/10/19	Mikel Fernández	References aligned with the split of D25-0015; §2 restructured against CRA Annex II point 8(f); support period, Article 14, VEX, release candidate and Debian update responsibilities added; editorial corrections

REFERENCES

Ref.	Title / Título
[1]	EU Cyber Resilience Act (Regulation EU 2024/2847) (Legal text)
[2]	Radio Equipment Directive (RED) Delegated Regulation (EU) 2022/30 (Legal text)
[3]	IEC 62443 Series of Standards (Standard)

[4]	EN 18031:2024 Harmonized Standard for RED Compliance (Standard)
[5]	D26-0006-D-PUBLIC-Owasys Release and Vulnerability Handling Policy

OWASYS CYBER RESILIENCE ACT (CRA) COMPLIANCE PATH AND SHARED RESPONSIBILITY MODEL

A Guide for System Integrators and Solution Developers on the Owasys Platforms

At Owasys, cybersecurity is a *shared responsibility* between the platform vendor and the integrator. Owasys gateways such as the owa4X and owa5X families are Open Platforms designed to run customer-developed software, which means that CRA compliance of the final product depends on contributions from both sides. This document describes how those contributions are divided.

Below is an overview of our compliance strategy, the artifacts Owasys provides, and how we divide responsibilities to ensure your final product succeeds in the EU and Global markets.

1 TARGET LEVEL OF CRA COMPLIANCE FOR OWASYS PLATFORMS

Owasys delivers platforms designed to meet the regulatory and technical security standards applicable to its product category. The Owasys hardware platform has already achieved **compliance with the Radio Equipment Directive (RED) Delegated Regulation (EU) 2022/30**. This compliance is formally validated through the CE marking of our products, backed by certification against the EN 18031 series of harmonized standards. This evaluation was successfully conducted and certified by an independent, internationally recognized third-party testing laboratory.

EN 18031 compliance covers a substantial subset of the requirements that the CRA will impose. Owasys uses this baseline as a starting point for CRA-specific work, focused on the gaps that EN 18031 does not cover (such as Art. 13 vulnerability handling and Art. 14 incident reporting).

In parallel, leveraging existing EN 18031 compliance, Owasys is aligning its Secure Product

Development Lifecycle with **IEC 62443-4-1**. Once the European Commission publishes the harmonised standards (hENs) for the CRA, Owasys is positioned to evaluate its platforms against **IEC 62443-4-2** (or the adopted European equivalent) to demonstrate technical component robustness.

The CRA general application date is 11 December 2027. The Owasys CRA preparation programme is structured to meet this date, with intermediate milestones tracked in the section Owasys CRA Compliance Roadmap.

1.1 CRA CLASSIFICATION

Under the CRA framework (Annex III), Owasys classifies its gateways as "**Important Products – Class I.**" Conformity may therefore be self-assessed where the harmonised standards are applied in full; otherwise a third-party assessment route applies.

2 DOCUMENTATION AND COMPLIANCE ARTIFACTS PROVIDED BY OWASYS

Owasys platforms are intended for integration into the final products of its customers. Annex II, point 8(f) of the CRA requires that such a product be accompanied by the information the integrator needs to comply with the essential cybersecurity requirements of Annex I and the documentation requirements of Annex VII. Owasys provides that information as follows. Items marked in preparation will be published in the Developers Zone.

Information	Relevant CRA provision	How it is obtained
Intended use definition and operational environment of the platform	Article 13(3); Annex VII, point 1(a)	Developers Zone (in preparation)
Platform cybersecurity risk assessment	Article 13(3); Annex VII	Summary: Developers Zone (in preparation). Full document: on request through the Developers Zone, under a non-disclosure agreement
Results of the platform evaluation against applicable harmonised standards (EN 18031 at present)	Annex VII	Summary statement: on request. Full results: on request, under a non-disclosure agreement
Security guidelines: recommended measures for commissioning, hardening and configuration	Annex II, point 8(a)	Developers Zone (in preparation)
Reference application built on the official Owasys BSP, as a secure baseline	Annex I, Part I	Developers Zone (in preparation)
Software bill of materials (SBOM) for each firmware release	Annex I, Part II, point (1)	On request
VEX report for each firmware release	Annex I, Part II	On request
Firmware releases with signed release manifest, release notes and update installation instructions	Annex I, Part II, point (7); Annex II, point 8(c)	Developers Zone

Information	Relevant CRA provision	How it is obtained
Security advisories and release security bulletins (bulletins introduced progressively)	Annex I, Part II, points (4) and (8)	Public section of the Owasys Security Centre
Vulnerability reporting contact and coordinated vulnerability disclosure policy	Annex II, point 2	Public section of the Owasys Security Centre
End date of the support period	Annex II, point 7	Quotation or order confirmation
EU declaration of conformity	Annex VII	Developers Zone (in preparation)

Parties without access to the Developers Zone may request the summary of the platform cybersecurity risk assessment under a non-disclosure agreement.

In addition, the Owasys engineering team supports integrators during the development, maintenance, and end-of-life phases of their solution.

3 THE OWASYS SHARED RESPONSIBILITY MODEL (SRM)

Because the Owasys platforms allow integrators to run custom applications, Owasys employs a Shared Responsibility Model. **Owasys secures the "Trusted Core" of the platform, while the integrator secures the custom application and its deployment.**

3.1 OWASYS RESPONSIBILITIES (*PLATFORM* SECURITY):

- Maintenance and support of the Board Support Package (BSP, including firmware, software components, toolchain, and documentation).
- Regular publication of firmware updates, including CVE analysis, security advisories and patches.
- Providing a dedicated CVE reporting channel for customers to report vulnerabilities.
- Notifying EU authorities (ENISA/CSIRTs) of actively exploited vulnerabilities and severe incidents affecting the security of Owasys products, in accordance with the CRA Art. 14 reporting timelines.
- Applying the Owasys end-of-line process to units supplied provisioned, so that no such unit leaves the factory on factory-default settings.
- Making remediation available, during the support period set out in the Owasys Release and Vulnerability Handling Policy [5], for vulnerabilities assessed as requiring it. Deploying it to a fleet is the integrator's responsibility; under a customer-managed trust chain Owasys is not technically able to deploy.

3.2 CUSTOMER/INTEGRATOR RESPONSIBILITIES (*APPLICATION* SECURITY):

- Defining the specific intended use of the final integrated product.
- Developing, testing, and maintaining the custom application software and settings.
- Securely provisioning the devices before deployment in production environments. Where units are supplied as **open units** (with base firmware and without the Customer end-of-line process) carrying out their own end-of-line and commissioning. An open unit is not fit for placing on the market until that has been done.
- Generating and protecting the RAUC signing keys where the integrator operates its

own PKI.

- Operating and maintaining the deployed devices in the field (e.g., applying the updates Owasys provides, configuring firewalls, managing passwords).
- Using release candidates for evaluation only, and not deploying them on devices in production.
- Reviewing and adapting the Owasys BSP, threat model, and risk assessment to ensure that the final integrated product placed on the market achieves full CRA compliance.
- Carrying out the conformity assessment of the final product.
- Determining the support period of the final product under CRA Article 13(8).
- Where the integrator places the final product on the market as its manufacturer, notifying actively exploited vulnerabilities and severe incidents affecting that product under CRA Article 14, and informing its own users. Owasys informs its direct customers only.
- Deploying available remediations for vulnerabilities in a timely manner, according to their specific operational environment and use case.
- Reassessing the Owasys VEX statements after any change to the firmware, its configuration or its exposed interfaces. Owasys statements apply to the firmware as released and to its intended use as documented by Owasys.

3.3 UPDATES ON DEBIAN-BASED FIRMWARE

On the Debian-based firmware line, Owasys consolidates the Debian updates published during each release period into its own release cycle and delivers them with the next Owasys firmware release. Where a Debian update addresses a vulnerability that Owasys routes to a security release, it is delivered outside the planned cycle, as described in the Owasys Release and Vulnerability Handling Policy [5].

This does not prevent integrators from applying Debian updates more frequently. Embedded devices, however, often operate unattended and may include components compiled from source with complex dependencies. Owasys therefore recommends that integrators evaluate these updates in the Owasys release candidates and deploy them with the stable firmware release. Debian updates applied outside an Owasys release are

not validated by Owasys; their validation is the responsibility of the integrator.

3.4 CUSTOMER REPORTING TO OWASYS

To support Owasys's own obligations under CRA Art. 14, integrators are expected to notify Owasys of:

- Any suspected or confirmed exploitation of an Owasys-supplied component on a deployed device.
- Any vulnerability discovered in an Owasys-supplied component during integration or operation.

Channels:

The reporting channels, the acknowledgement commitment, the PGP key fingerprint and the coordinated disclosure policy are published in the public section of the Owasys Security Centre. That page is the single source for them; this document does not duplicate it.

4 OWASYS CRA COMPLIANCE ROADMAP

Owasys has identified two regulatory milestones for the CRA:

- **11 September 2026** - Art. 14 vulnerability and incident reporting obligations apply. The governance, the notification procedure, the 24-hour and 72-hour timelines and the final-report deadlines are documented in the Owasys Release and Vulnerability Handling Policy [5], with advisories published in the public section of the Owasys Security Centre, and release security bulletins introduced progressively.
- **11 December 2027** - CRA general application. Owasys is aligning its Secure Product Development Lifecycle with IEC 62443-4-1 and will evaluate platform component robustness against IEC 62443-4-2 once the CRA harmonised standards are published.

Owasys's CRA compliance path for its products is well underway, with internal procedures and tooling being deployed in parallel with the regulatory timeline. Customers are encouraged to engage early through the channels listed in the section Customer reporting to Owasys or through your usual Owasys sales representative.

The Owasys team is available to discuss specific integration scenarios as your CRA compliance work progresses.