CRA SAMPLE

Procedure: networked wood chip heating

Under the Machinery Regulation and the Cyber Resilience Act

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Example	Nordwald Wärmetechnik GmbH (fictitious), two people
Note	Free sample, not legal advice

Companies, people and data are fictitious. Real products serve only as a technical reference.

1 How to use the procedure

Work through the nine steps in order. For each step the matching documents exist twice: as a blank template and as a filled example for Nordwald Wärmetechnik GmbH. All files: ot-cyber.de/en/examples/cra-wood-chip-heating/

1.1 The example

Nordwald Wärmetechnik GmbH (fictitious) consists of two people: Michael Berger, master heating engineer and managing director, and Jonas Weiß, mechatronics technician specialising in control engineering. The company places the wood chip boiler NWT HACKTHERM 60 connect (18 to 60 kW, boiler class 5) on the market under its own brand and is therefore the manufacturer. Production and development are done with partners.

Partner	Contribution
Kesselbau Alpenrand GmbH	Boiler body, room discharge, rotary valve
Schaltanlagen Hofer GmbH	Control cabinet, routine test
Datenwerk Embedded GmbH	Gateway, portal, app, SBOM, updates
Ingenieurbüro Lechner	Safety functions, validation
Sichtwerk Security GmbH	Penetration test, on-call duty for reports
Prüfinstitut Feuerungstechnik Süd	Type test EN 303-5, EMC

Partners deliver services. The obligations under the Machinery Regulation and the CRA stay with the manufacturer and are secured by contracts, reporting routes and evidence (D02, F03).

1.2 Deadlines

When	What
11 Sep 2026	Reporting obligation under Article 14 CRA applies already, also for networked plants that have been delivered before.
until 19 Jan 2027	Machinery Directive 2006/42/EC with EC declaration of conformity.
from 20 Jan 2027	Machinery Regulation (EU) 2023/1230, without a sell-off period.
from 11 Dec 2027	CRA applies in full, CE marking also under the CRA.

2 Step 1: Classify

Do the Machinery Regulation and the CRA apply, and are we the manufacturer?

Who: Berger (managing director), checked by Weiß · In the example: Nov 2026

1. We are affected because we create an assembly of machinery: several machines arranged and controlled so that they work together as one plant. The boiler with its motor-driven augers alone is already a machine. This makes us the manufacturer under the Machinery Regulation. When we hand the plant over to the customer, we place this assembly on the market. Because it is networked, it is a product with digital elements and also falls under the CRA.

2. Fix the legal acts and dates: Machinery Regulation from 20 January 2027, CRA in full from 11 December 2027, reporting obligation since 11 September 2026.

3. Determine the CRA class: core function heat generation, no category in Annex III or IV, so a default product.

4. Choose the conformity assessment procedure: internal control under both legal acts, no notified body.

2.1 Which role do we have? Three cases

Case A: own name or own brand. The plant goes to the customer under our name or brand, even if partners make parts of it.

Machinery Regulation: full manufacturer obligations. CRA: full manufacturer obligations.

Case B: assembly of machinery, without an own product brand. We combine boiler, room discharge system, rotary valve and controller from different suppliers into one plant and hand it over in working order at the customer site. For us this is the decisive reason; our own brand comes on top.

Machinery Regulation: manufacturer of the assembly, own name on the rating plate, own declaration. CRA: manufacturer of the whole plant if it is networked; for controller and gateway we rely on the suppliers' declarations, SBOMs and updates.

Case C: installing finished devices without modification. We install a finished, CE-marked device according to the manufacturer's instructions, without combining it with other machines into one plant and without changing software or security settings.

No manufacturer obligations, only distributor and installation duties. Anyone who switches off safety functions, sets up remote access on their own or changes software has to check again: this can be a substantial modification.

It does not matter whether the plant is assembled in our workshop or at the customer site. A plant used only in your own company does not fall under the CRA, but it does fall under the Machinery Regulation. How authorities view assembly at the customer site in an individual case has not been finally settled; agree the manufacturer role in writing with the customer and the suppliers.

Result: Matrix of legal acts, list of standards and assessment procedure are fixed.

No.	Document	Template and example
D01	Classification, legal framework and assessment procedure	blank and filled

3 Step 2: Set up the company

How do two people cover all manufacturer obligations?

Who: Berger, Weiß, partner companies · In the example: Nov 2026

1. Allocate roles with deputies: management and CE with Berger; engineering, safety and product security with Weiß.

2. Bind partners by contract: reporting routes, 15-year support commitment, retention, source code escrow.

3. Become able to report: access to the ENISA single reporting platform, on-call duty, emergency card, reporting drill.

4. Plan and record training.

Result: The organisation is in place; the company can report vulnerabilities and incidents on time.

No.	Document	Template and example
D02	Roles, subcontractors and allocation of obligations	blank and filled
D16	Emergency card: reporting under Article 14 CRA	blank and filled
F03	Subcontracting agreement: CRA and MR annex	blank and filled
F06	Reporting record under Article 14 CRA	blank and filled
F12	Training record	blank and filled

4 Step 3: Describe the plant

What exactly do we place on the market, and for what purpose?

Who: Weiß, approval by Berger · In the example: Dec 2026

1. Record product data, assemblies and interfaces.

2. Describe intended use and reasonably foreseeable misuse, including remote access.

3. Define limits and life phases, including updates and decommissioning.

4. Enter requirements with their source in the requirements list.

Result: Plant description and requirements list as the basis for all further steps.

No.	Document	Template and example
D03	Plant description	blank and filled
F01	Requirements list	blank and filled

5 Step 4: Design for safety and security

How does the heating system stay safe, even under attack?

Who: Weiß with engineering office and software partner · In the example: Dec 2026

1. Select a safety controller certified to IEC 62443-4-2.

2. Define safety functions SF1 to SF10 with their required performance level (PLr).

3. Principle: safety temperature limiter, thermal discharge safety device, safety valve and extinguishing work without software and without the network.

4. Plan zones and conduits according to IEC 62443, remote maintenance only after approval, signed updates.

Result: Control and safety concept and network architecture.

No.	Document	Template and example
D04	Control and safety concept	blank and filled
D05	Network and system architecture	blank and filled

6 Step 5: Assess the risks

Which hazards remain, and are they acceptable?

Who: Weiß, Berger, engineering office, security partner · In the example: Jan 2027

1. Assess hazards according to EN ISO 12100 for all life phases and reduce them with the three-step method.

2. Assess cyber threats according to IEC 62443-3-2 and map them to CRA Annex I.

3. Show that an attack cannot defeat a safety function (MR Annex III, sections 1.1.9 and 1.2.1).

4. Record residual risks for the instructions.

Result: Two risk assessments with a joint cyber safety argument.

No.	Document	Template and example
D06	Risk assessment, machinery safety	blank and filled
D07	Cybersecurity risk assessment	blank and filled

7 Step 6: Introduce processes

What has to run permanently in the company?

Who: Weiß (PSO), Berger, software partner · In the example: Dec 2026 to Mar 2027

1. Introduce 20 processes according to the process manual: development, SBOM, vulnerabilities, updates, changes, market surveillance.

2. Assess suppliers and components.

3. Publish the coordinated vulnerability disclosure policy and security.txt.

4. Ship every release with an SBOM and a security approval.

Result: Processes that are actually lived, with evidence for the technical documentation.

No.	Document	Template and example
D08	Process manual	blank and filled
D14	Coordinated vulnerability disclosure policy	blank and filled
F02	Supplier and component assessment	blank and filled
F04	SBOM release	blank and filled
F14	Security release approval	blank and filled

8 Step 7: Test and validate

Does everything work as planned?

Who: Weiß, engineering office, test laboratory, partners · In the example: Jan to Mar 2027

1. Type test to EN 303-5 and EMC at an accredited laboratory.

2. Validate every safety function with fault injection.

3. Penetration test and communication failure test.

4. Introduce a routine test for every serial number.

Result: Test reports, validation records, routine test record.

No.	Document	Template and example
F09	Validation record, safety function	blank and filled
F10	Routine test record	blank and filled

9 Step 8: Document and declare

What is needed for the CE marking?

Who: Berger (signature), Weiß · In the example: Mar 2027

1. Compile the complete technical documentation.

2. Publish the user information, with the simplified EU declaration of conformity under Annex VI and the end of the support period for each unit (15 years from handover).

3. Work through the checklist, then sign the joint EU declaration of conformity: with the statement that fulfilment of Annex I has been demonstrated, valid from 11 December 2027, and standards with their edition.

4. Attach the rating plate, CE marking and end-of-support label.

Result: Signed declaration, CE marking, release for placing on the market.

No.	Document	Template and example
D09	Technical documentation: table of contents	blank and filled
D10	Checklist before placing on the market	blank and filled
D11	EU declaration of conformity	blank and filled
D12	Rating plate and marking	blank and filled

No.	Document	Template and example
D13	User information under CRA Annex II	blank and filled
D15	Support period statement	blank and filled

10 Step 9: Deliver and support

What applies after the sale, over the whole support period?

Who: Weiß (service, PSO), Berger · In the example: from Mar 2027

1. Commissioning with a secure initial configuration.
2. Handle vulnerabilities, inform users, provide updates free of charge.
3. Check changes for substantial modification.
4. Carry out corrective actions and inform authorities where required.

Result: Conformity and safety over the entire support period.

No.	Document	Template and example
F05	Vulnerability ticket	blank and filled
F07	Security advisory to users	blank and filled
F08	Change request	blank and filled
F11	Commissioning record	blank and filled
F13	Corrective action and contact with authorities	blank and filled

11 Important notes

• The sample documents are internal evidence. The declaration of conformity lists legal acts, standards and specifications; a presumption of conformity only arises from harmonised standards cited in the Official Journal.

• As of 5 November 2026 there is no cited harmonised standard yet for the CRA or for MR Annex III, section 1.1.9. IEC 62443, EN 40000-1-2 and FprEN 50742 are used as specifications and the solutions are justified in the documentation.

• Risk figures, PL values, deadlines and support duration are justified sample values. Every manufacturer assesses its own product.

• Microenterprises and small enterprises are not fined for missing the 24-hour early warning deadline. The reporting obligation itself still applies (Article 64(10)(a) CRA).

• Before every declaration, check the status of the Official Journal, standards and national implementation acts.

All templates and examples: ot-cyber.de/en/examples/cra-wood-chip-heating/ · Free sample by OT-Cyber.de, not legal advice.