CRA SAMPLE

D07 Cybersecurity risk assessment

Blank template · Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Sample company	Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect (fictitious)
Note	Free sample, not legal advice

Fill in the fields, approve with date and signature, file according to document control.

1 Purpose and scope

Risk assessment under Article 13 CRA and IEC 62443-3-2, with evidence for MR Annex III, sections 1.1.9 and 1.2.1: no attack via the network or portal can defeat a safety function. R = L × I, acceptable up to 4.

How to fill in this form

Fill in the fields with the details of your company. Below each table and next to each field there is an example from the sample company for orientation. Refer to evidence by number (e.g. ticket or form). Finally approve with date and signature and file according to document control.

2 Document control

Field	Entry
Document no.	
Version, status	
Scope	
Author	
Checked by	
Approval	
Next review	
Confidentiality	
Filing	

3 Scope of the assessment

Field	Entry	Example from the sample
Intended use		Heat generation in the boiler room, remote …
Operating environment		Boiler rooms in commercial, municipal, …
Assets		Safety functions SF1 to SF10, F program, …

Field	Entry	Example from the sample
Service life		15 to 20 years per boiler; threats assessed …
Method		R = L × I, L and I each 1 to 4; acceptable up …
Annex I, Part I		For each of points (2)(a) to (m), F01 records …

4 Threats and measures

How to read the table

Each row is a threat to the boiler, gateway, portal or app. R0 is the risk without measures, R1 the risk with measures, in each case likelihood times impact, both rated from 1 to 4. Any R1 above 4 requires further measures. The Reference column shows which CRA requirement the measure fulfils.

ID	Threat	Path	R0	Measures	R1	Reference

Example row from the sample: ID: C01 · Threat: Customer account takeover · Path: Internet · R0: 9 · Measures: MFA, rate limiting · R1: 4 · Reference: I 2 d

Legend: C = cyber threat; R0 = risk before measures; R1 = risk after measures, R = L × I with L = likelihood 1 to 4 and I = impact 1 to 4, acceptable up to 4; Reference = CRA requirement, e.g. "I 2 d" = Annex I, Part I, point (2)(d).

Describe your status here, specifically and with a date. Example from the sample: C14 remains at 4: the key is stored in the HSM and used only under the four-eyes principle; a lower value cannot be achieved with reasonable effort.

5 Cyber safety evidence

Describe your status here, specifically and with a date. Example from the sample: Worst case: an attacker has full control of the portal and gateway.

Assessment round	Trigger	Result

Assessment round	Trigger	Result

Example row from the sample: Assessment round: 28.06.2027 · Trigger: NWT-VULN-2027-004 (MQTT library) · Result: C12 confirmed, daily monitoring

6 Terms and abbreviations

CRA: Cyber Resilience Act, Regulation (EU) 2024/2847

HSM: hardware security module, protects the signing keys

LAN: local area network

MFA: multi-factor authentication

MQTT: messaging protocol between device and portal

MR: Machinery Regulation (EU) 2023/1230, applies from 20 January 2027

NWT: abbreviation of the sample company in document and ticket numbers

SBOM: software bill of materials: which components in which version

SF: safety function

TLS: encryption of the connection

USB: USB port

VULN: vulnerability ticket (number range)

7 Revision history and approval

Version	Date	Change	Approval

Approved (name, function, date, signature): _____ · Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.