CRA SAMPLE

# F02 Supplier and component 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

Due diligence for third party components (Article 13(5) CRA): assessment of suppliers and components with regard to security, support throughout the support period and vulnerability status. Annually and on change (P05).

**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 Supplier and component assessment: overview

| Component | Supplier | Support until | Vulnerabilities 2027 | Rating |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Example row from the sample: Component: Safety controller · Supplier: Controller manufacturer · Support until: 2037, successor planned · Vulnerabilities 2027: 1 medium, patched · Rating: A

| Field | Entry | Example from the sample |
|---|---|---|
| Criteria | | Supplier's security process, origin and … |
| Rating | | A without conditions, B with conditions, C not … |
| Conditions B | | MQTT library: daily monitoring, replacement … |

# 4 Terms and abbreviations

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

**HSM:** hardware security module, protects the signing keys

**MQTT:** messaging protocol between device and portal

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

**TLS:** encryption of the connection

**VULN:** vulnerability ticket (number range)

# 5 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.