



# Cyber Resilience Act

From regulatory requirement to assessable reality

Industrial Security - CRA · 29.09.2026  
Florian Schmidt, TÜV SÜD Product Service

**Mehr Wert.  
Mehr Vertrauen.**

# Who's speaking – and why we can speak plainly

Assessment body, not sales



## Florian Schmidt

**Senior Cybersecurity Expert, TÜV SÜD  
Product Service**

- Testing connected products: RED / EN 18031, CRA, IEC 62443
- Before: machinery engineering, automotive safety & security
- Standardisation work

*"I know both sides of the test bench."*

## Why plain talk is possible

- Independent assessment body – we sell no security products
- Assessments across sectors: machinery, IoT, building tech
- Every statement today is a real project observation

**Questions any time – no Q&A jam at the end.**

→ **Neutrality is the licence to speak plainly.**

**“Paper doesn’t beat anyone –  
assessors want evidence.”**

Processes on paper: almost everywhere. Robust evidence: almost nowhere.

# The evidence triad

An assessor accepts all three levels – not just one



## Documentation

What you say you do

- Risk assessment
- Testable requirements
- Architecture, SBOM
- Support period

## Lived process

What you really do

- Dated reviews
- Change process
- PSIRT tickets, CVD cases
- Roles, training

## Technical test

What the product can do

- Test reports per requirement
- Pentest with retest
- SBOM ↔ CVE scan
- Hardening evidence

Docs without test = claim · test without process = chance · process without docs = not assessable

→ Paper doesn't beat anyone – assessors want evidence on all three levels.

# Three types of evidence – what each proves, what not

Verification & validation · penetration test · vulnerability analysis



## Security V & V

Proves: every requirement was tested as planned – functional tests, reviews, analyses

Does not prove: that an attacker finds no other way

## Penetration test

Proves: what a motivated attacker achieves in scope within limited time

Does not prove: completeness – a pentest without findings means too small a scope

## Vulnerability analysis

Proves: known vulnerabilities in components (SBOM ↔ CVE), configuration, hardening

Does not prove: logic flaws and unknown vulnerabilities

→ No evidence replaces another – an assessor wants all three, with scope and date.

# Anatomy of a robust test report

Six elements – if one is missing, the report fails in the assessment



1

## Scope

Product, firmware version, interfaces, test period, tester

2

## Method

Approach, tools, reference (e.g. OWASP, EN 18031 test methods)

3

## Findings with severity

Each finding with CVSS, reproduction steps, evidence

4

## Retest

What was closed, what accepted – with rationale and signature

5

## Mapping

Findings → requirements (SR-xx) → risks (R-xx)

6

## Approval

Version, date, owner – linked in the technical documentation

→ Page count doesn't matter – scope, findings, retest and mapping do.

# Evidence reality check: the pentest report

Page count doesn't matter – scope, findings, retest, mapping do



anonymised

## FAILED – “pentest passed”, 2 pages

### What the report says

- Scope: “the device” – no version, no interfaces
- “No critical vulnerabilities found.”
- No methodology, no findings list
- No retest, no link to requirements

## HOLDS – pentest report, 38 pages

### What the report says

- Scope: FW 2.3.1, web UI, BLE, MQTT, maintenance port
- OWASP methodology, 11 findings with CVSS
- Retest: 9 closed, 2 accepted with rationale
- Mapping findings → requirements → risks

→ A pentest without findings isn't a good sign – but a sign of too small a scope.

# The first five questions of every assessment

And how we recognise a good answer

Audit  
view



## ASSESSOR QUESTION

1

“Show me your risk assessment – who last changed it?”

2

“Which requirement treats risk no. 7 – where is the test?”

3

“What’s inside your product?”

4

“How does a researcher reach you – what happens in 24 hours?”

5

“How long do you support the product?”

## GOOD ANSWER

Versioned, with criteria, newer than the last release

Risk → SR-xx → test report in one table

SBOM from the build, all levels, CVE matching

CVD policy online, roles, one documented case

Support period defined and published

→ Answer these five questions in ten minutes and you’ve got the basics right.

# Gaps between claim and reality

Six findings that keep recurring in assessment projects



## Gap 1

### SBOMs unworthy of the name

Hand-kept lists, low coverage, no versions.

## Gap 2

### Risk analyses for the auditor

Generic, not product-specific, written after design.

## Gap 3

### Requirements no one can test

“The product must be secure” – no criterion, no method.

## Gap 4

### Channel without a decision

security@ exists – but nobody decides within 24 h whether to report.

## Gap 5

### Support period, no plan

Period set – but no plan for who delivers updates to the end.

## Gap 6

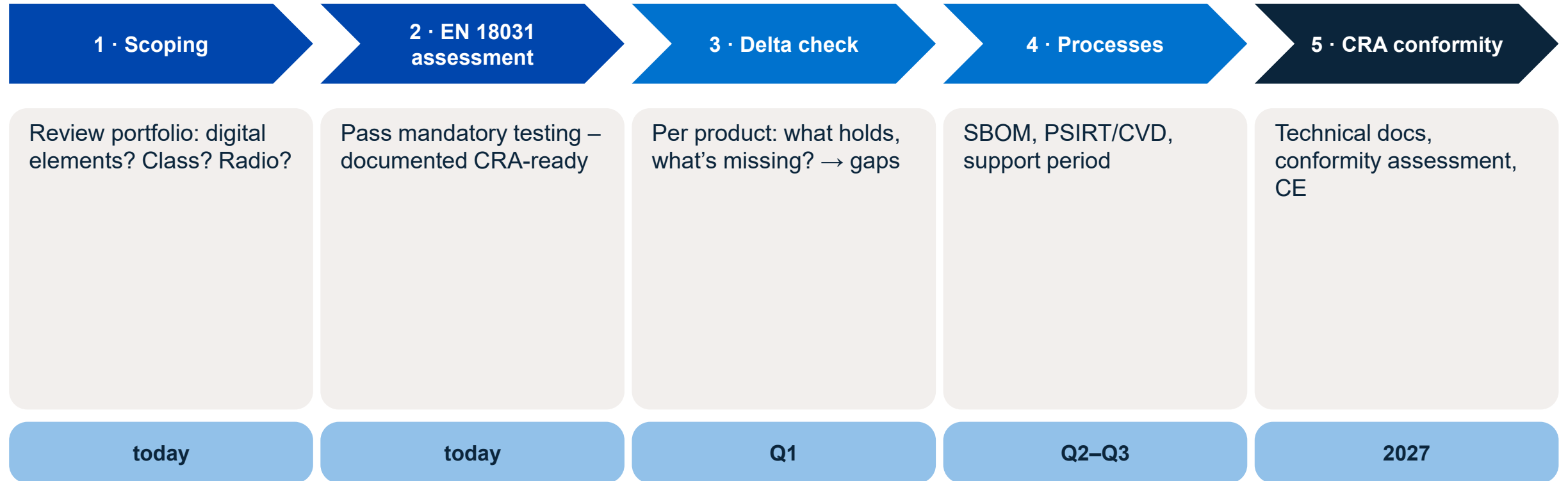
### Docs without version

Test reports, risk analysis and SBOM can't be traced to a release.

→ The claim lives in the process manual – assessed is the reality in the evidence.

# Crossing the bridge – five steps

From RED duty today to CRA conformity 2027



→ RED is your chance to lay the foundation for CRA conformity today.

# The CRA doesn't start with the audit – but with the decisions developers make today.

“Everyone is affected by the CRA – no one is ready.” Now you know where to start.



## Contact

**Florian Schmidt**

Senior Cybersecurity Expert

TÜV SÜD Product Service  
GmbH

[Florian.Schmidt@tuvsud.com](mailto:Florian.Schmidt@tuvsud.com)