

Cyber Resilience Act: hands-on

What manufacturers must do today to pass tomorrow

IT-SECX – 02.10.2026 · 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 (DKE)

“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.**

“The CRA affects everyone – no one is ready.”

No marketing claim. Our daily testing.

Live check: where do you stand?

Three questions for you

1

Do you make products with digital elements?

Controller, radio, app, cloud, firmware

2

Do you have a complete SBOM for them?

All layers, with versions, from the build

3

Can anyone test your security requirements?

Measurable, with a test method

How are things with you?

Who is affected – and who isn’t

Products with digital elements – hardware and software

Affected

- Every product with digital elements that can be connected
- Hardware and software: machine, sensor, app, firmware
- B2B and B2C – component and end product
- Manufacturers, importers, distributors, own-brand integrators

Excluded

- Type-approved vehicles
- Medical devices (MDR / IVDR)
- Civil aviation, marine equipment
- National security, defence

Special cases

- In principle only commercial products
- Pure SaaS: NIS2, not CRA
- Spare parts: exempt if identical
- Substantial modification: manufacturer again

→ **Affected: whoever places a product with digital elements on the market – not just software vendors.**

Your obligations on one page

Annex I as a map – each further slide zooms into one field

Annex I – Essential cybersecurity requirements

Part I – Product properties (13)

Security by design & default · access control · updates · logging · data minimisation

Part II – Vulnerability handling (8)

SBOM · fix vulnerabilities · tests · CVD · reporting · secure, free updates

Risk assessment
Art. 13 – the basis of it all

Technical docs
Annex VII + user info Annex II

Reporting
Art. 14 – since 11 Sep 2026

Conformity & CE
Art. 32, Annex VIII

Applies across the whole life cycle – until end of support

→ **One page, all obligations – no clause marathon, but no shortcut either.**

Evidence reality check: the SBOM

If you don’t know what’s in the product, you can neither secure nor report

anonymised

30 %

Coverage – hand-kept Excel list

100 %

per release – automatically from the build

Before

- Only top-level libraries, no versions
- Firmware base (RTOS, bootloader) missing
- 14 months out of date
- On a CVE: nobody knows if affected

After

- SBOM-Tool in the toolchain
- All levels, versions, licences
- Automatic CVE matching → PSIRT
- Effort: minutes per release

→ The SBOM isn’t a document but a build artefact – maintain it by hand and you don’t have one.

Same company, six months later

Risk analysis before / after – the difference is product focus

anonymised

BEFORE – written for the auditor

Risk analysis product family X – sect. 4.2

Risk 3: cyber attack on the device.

Likelihood: medium. Impact: medium. Class: II.

Measure: state of the art is followed.

Residual risk: acceptable.

AFTER – written for the product

Risk assessment ThermoLink v2.3 – R-07

Asset: OTA channel · threat T-03: tampered firmware

Likelihood: medium (from LAN) · impact: high (full access)

Risk HIGH → unacceptable (criteria v1.2)

Treatment: SR-12 · evidence: TR-04, PT-02

Why this doesn't hold

- No product link – which interface?
- No criteria – "medium" is not justified
- Measure not verifiable

Why this holds

- Specific asset, specific threat
- Justified against dated criteria
- Linked to requirement and evidence

→ Same effort – the right describes a product, the left fills in a form.

Problem area: requirements nobody can test

Finding from assessments – and how it becomes a test criterion

fictitious

Finding: security objectives instead of requirements – no actor, no criterion, no method.

	UNTESTABLE	TESTABLE
Authentication	*“Access for authorised users only.”*	Login only with password ≥ 12 chars or certificate; factory password must be changed.
Updates	*“Updates must be secure.”*	Only firmware with valid signature (ECDSA P-256); unsigned images are rejected.
Logging	*“Events are logged.”*	Failed logins, config and update events timestamped, ≥ 30 days.
Cryptography	*“Data is encrypted.”*	App ↔ device TLS 1.3 only, with pinning; plaintext fallback disabled.

→ Testable means: actor, condition, criterion, method – and an assessor can say yes or no.

Art. 14 reporting: the deadlines

In force since 11 Sep 2026 · two strands, one clock

Actively exploited vulnerability



Severe incident



Where: Single Reporting Platform (ENISA) → competent CSIRT · inform affected users without delay

The clock starts on awareness – not on verification, not on the patch.

→ **The question isn't whether Art. 14 applies – but whether you could decide in 24 hours today.**

Outward: CVD policy · inward: PSIRT roles

The rules for reporters – and the people who decide within 24 hours

CVD = Coordinated Vulnerability Disclosure – the public rules for anyone who finds a vulnerability in your product: where to report? What happens next? Must I fear legal action? The CRA requires such a policy (Annex I Part II No. 5).

What belongs in the CVD policy

- Channel: security@ and security.txt – publicly findable
- Promise: receipt within 2 working days, status every 14 days
- Safe harbour: no legal action against good-faith reporters
- Coordinated disclosure: deadline, advisory, CVE number

PSIRT = Product Security Incident Response Team

- **PSIRT lead: decides on reporting, keeps the clock**
- Triage: reproduces, rates, checks exploitation
- Development: fix, test, release · Comms: customers, advisory, authority
- **Who decides on Friday evening? Every role needs a deputy.**

→ **A process only becomes one when every role has a name – and a deputy.**

The first five questions of every assessment

And how we recognise a good answer

Audit view

	ASSESSOR QUESTION	GOOD ANSWER
1	**“Show me your risk assessment – who last changed it?”**	Versioned, with criteria, newer than the last release
2	**“Which requirement treats risk no. 7 – where is the test?”**	Risk → SR-xx → test report in one table
3	**“What’s inside your product?”**	SBOM from the build, all levels, CVE matching
4	**“How does a researcher reach you – what happens in 24 hours?”**	CVD policy online, roles, one documented case
5	**“How long do you support the product?”**	Support period defined and published

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

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.

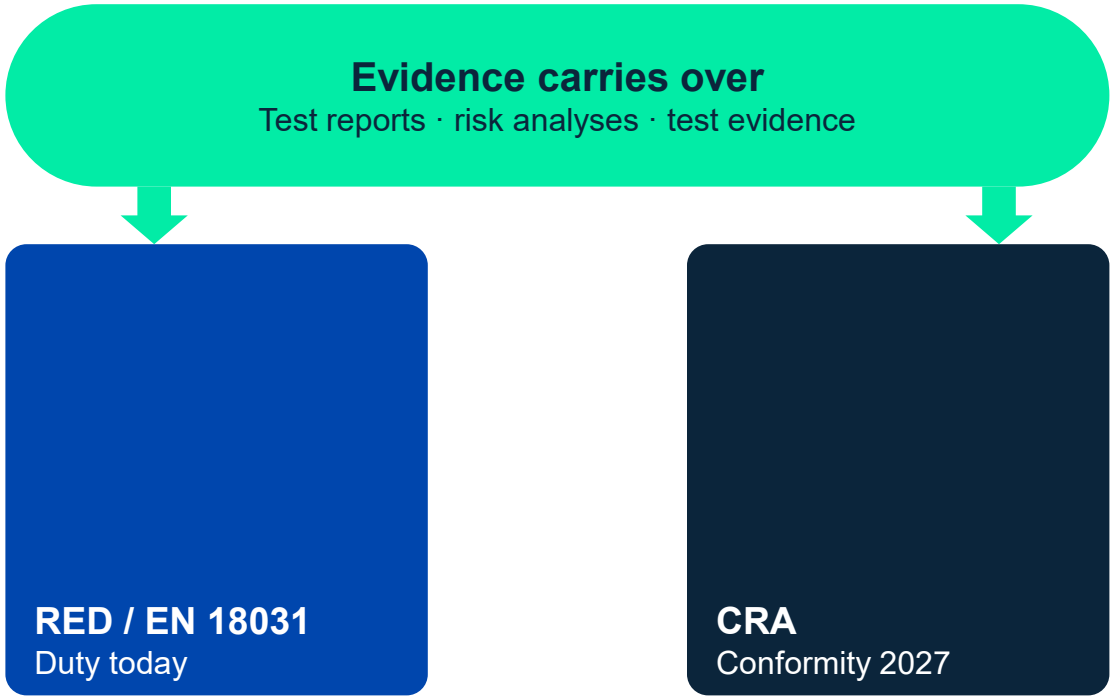
The bridge from RED to CRA

Passed EN 18031 testing? You're not starting from zero

Head start, not double work

Today's RED duty is the cheapest entry into the CRA – documented CRA-ready, the 2027 test file is half full.

RED testing today → CRA documentation 2027



Specifics

- EN 18031 tests today what the CRA needs tomorrow
- RED evidence is CRA evidence – if documented CRA-ready

→ Leave the evidence unused and you test twice in 2027.

Your next 12 months

Four quarters – each ends with evidence

Week 1 **Quick wins**	Q1 **Inventory & gap**	Q2 **Processes**	Q3 **SDL & testability**	Q4 **Rehearsal**
▪ security@ + security.txt ▪ Product list with class ▪ Review RED reports	▪ SBOM from the build ▪ Class per product ▪ Delta check	▪ Risk assessment ▪ PSIRT/CVD with roles ▪ Support period	▪ Requirements testable ▪ Verification plan ▪ Change process	▪ Technical docs ▪ Audit simulation ▪ Close remaining gaps
Evidence: **Owner appointed**	Evidence: **Gap list prioritised**	Evidence: **First drill**	Evidence: **Test reports with mapping**	Evidence: **Technical docs audit-ready**

→ **Order matters more than speed.**

Five things that can be done next week

No budget, no project proposal

1. **Set up security@ + security.txt**
   One person reads daily. Name a deputy.

2. **Create list of products with digital elements**
   Product, interfaces, radio yes/no, class, RED tested?

3. **Review RED / EN 18031 reports**
   First delta list on one page.

4. **Make five requirements testable**
   Discuss with the team.

5. **Try an SBOM tool in the build**
   Add a SBOM plugin to one product.

→ **Five Days – and you'd have good answers to three of the first five assessment questions.**

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