



CYBER RESILIENCE ACT · REGULATION (EU) 2024/2847

Making the Cyber Resilience Act work for SMEs

Evidence from the CYBERFORT project and ten actions for national and EU authorities before the CRA applies in full on 11 December 2027.

2 → 21

of 30 CRA objectives met after one remediation sprint

≈ 90%

less effort to draft a CRA policy with automated tools

94%

of SME workshop respondents asked for more support

14

months left until all CRA obligations apply

Key messages

1 The clock is running

Reporting obligations have applied since 11 September 2026. All essential requirements apply from 11 December 2027, while harmonised standards are still being finalised.

2 The gap is process, not technology

The blockers were missing disclosure policies, SBOMs, update routines and technical files. Once made visible, one manufacturer went from 2 to 21 of 30 CRA objectives met in one sprint.

3 Tools work with hands-on support

Automated drafting cut the effort for a CRA policy by about 90%. Webinars built reach; workshops and one-to-one sessions built capability.

4 What we ask for

A national CRA support package for SMEs before December 2027, built on what already exists: the NCC, the EDIH network, EU-funded open-source tools and EU cascade funding.

The problem

The CRA makes every manufacturer of a product with digital elements responsible for its security across the product's life. Its obligations arrive in stages, and the hardest one is 14 months away.

10 Dec 2024

Entry into force

11 Sep 2026

Reporting via ENISA platform

11 Dec 2027

Applies in full



Standards arrive late

None is yet cited in the Official Journal, so none yet gives a presumption of conformity.

Guidance is new

The Commission's guidance dates from 27 July 2026 and is not yet available as national, sector-specific material in Romanian.

The work is organisational

Vulnerability handling needs routines and people: a security contact, a disclosure policy, an SBOM, a technical file.

What CYBERFORT found

CYBERFORT (December 2024 – July 2026) built an open-source CRA compliance platform for SMEs and tested it in maritime, finance, energy and cybersecurity-product pilots.

Making gaps visible moves readiness fast

CRA objectives, of 30 · manufacturer pilot

Baseline

2

10

18

After one sprint

21

8

1

■ Compliant ■ Partial ■ Not compliant

The one objective left needs a notified body, which no engineering work can replace.

Automation cuts the paperwork

Effort to produce one CRA policy, person-days

Manual drafting

4–5

With CYBERFORT

■ ≈ 0.5 review

The finance pilot reached compliance readiness in about 3 months instead of 6 or more.

SMEs want hands-on help

“CRA Ready for SMEs” online workshop, 10 June 2026

Registered

192

Attended

122

Answered

88

94% of respondents asked for more CYBERFORT activities

The blockers were routines, not scanners

No coordinated disclosure policy

No security contact

No SBOM

No security-update policy

Incomplete technical file

All five sit in Annex I Part II, vulnerability handling. Critical-infrastructure customers already expect this evidence from their suppliers, which pushes the requirement down to SMEs.

60

organisations on the platform

160

users by 30 September 2026

1,677

policies generated

4

sector pilots validated

Ten actions before December 2027

The first five are national and can start in the first quarter of 2027 with existing institutions and funds.

NATIONAL AUTHORITIES

01 A Romanian CRA guide for SMEs

By March 2027: scope, product class, the 24 h / 72 h / 14-day reporting steps and the vulnerability-handling routines.

02 One CRA help point for SMEs

Through the National Coordination Centre and the EDIHs, with referral to the competent national authorities.

03 A reporting-readiness exercise

Manufacturers and the national CSIRT test the Single Reporting Platform before a real report is due.

04 Channel SMEs to CRA funding now

Promote the SECURE call before 11 December 2026; fund through EDIH or national programmes what it does not reach.

05 Recommend free, open-source compliance tools

Include EU-funded tools such as CYBERFORT in national awareness material, without endorsing commercial products.

EU BODIES · COMMISSION, ECCC, ENISA

06

Templates over text

Model disclosure policies, SBOM and support-period statements, technical-file and declaration skeletons for micro-enterprises.

07

Keep open tools alive

Fund maintenance of open-source compliance tools after Digital Europe grants end, in one catalogue across the NCC network.

08

CRA in the Skills Academy

Add CRA modules to the EU Cybersecurity Skills Academy, using ECSF-aligned material such as the CYBERFORT Academy.

SUPPORT ECOSYSTEM · NCCs, EDIHs, ASSOCIATIONS

09 Pair every webinar with hands-on follow-up

A workshop, a clinic or a one-to-one assessment: reach alone does not change readiness.

10 Reach SMEs through their customers

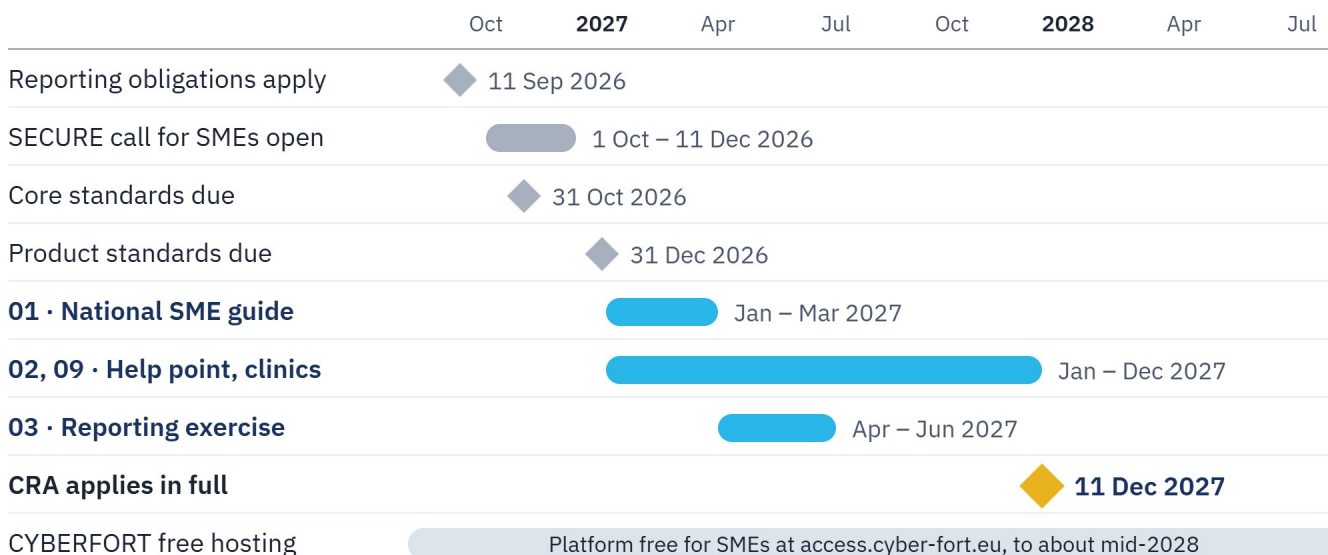
Align critical-infrastructure supplier requirements with CRA evidence, using NIS2 supply-chain duties as the lever.

National support must run in 2027

The guide and help point need to be in place in the first half of 2027 to leave SMEs time to act before 11 December 2027.

■ Recommended national action

■ Date set by the CRA or an EU measure



Who should receive this brief

Recipient	Why	Actions
Ministry responsible for digitalisation	National CRA implementation and funding	1, 4, 5
CRA market surveillance authority, national CSIRT	Guidance, help point, reporting exercise	1, 2, 3
ANCOM	Overlap with radio-equipment and AI surveillance	1, 2
Romanian EDIHs	Help point and hands-on follow-up	2, 4, 9
SME and software associations, chambers	Reaching SMEs; supplier alignment	4, 9, 10
DG CONNECT, ECCC, ENISA	EU templates, tool maintenance, skills	6, 7, 8
NCC network, STRENGTHENCRA, SECURE, CRA Cluster	Reuse of tools and material	7, 9